Francesc Bars Cortina

Unes nocions de Matemàtica Discreta.

Apunts de classe:
Grau en Matemàtiques
UAB, 26 de febrer de 2026
Curs 2024/2026.

Contingut

Capítol 1

Conjunts discrets, consideracions generals

1.1 Una noció de conjunt discret

Un valor absolut en un cos K o un anell commutatiu (sempre $1 \neq 0$) és una aplicació:

$$|\ | : K \to \mathbb{R}_{\geq 0}$$

complint les condicions següents:

Donat $k \in K$:

1. $|k| = 0 \Leftrightarrow k = 0$,
2. $|x + y| \leq |x| + |y|$, $\forall x, y \in K$
3. $|x \cdot_k y| = |x| \cdot_{\mathbb{R}} |y|$, $\forall x, y \in K$.

Un valor absolut en k es diu no-arquimedià si satisfà a més que $|x + y| \leq maxim(|x|, |y|)$ $\forall x, y \in K$.

Un valor absolut en K defineix una distància en K via:

$$dist(x, y) := |x - y|.$$

Definició 1.1. *Un conjunt $U \subseteq K$ s'anomena discret respecte la topologia $||$ si per a cada $u \in U$ existeix un nombre real $\epsilon_u > 0$ (escrivim $B_{\epsilon_u}(u) := \{k \in K : t.q. |k - u| < \epsilon_u\}$ denota la bola oberta centrada en u de radi ϵ_u), on es compleix que*

$$B_{\epsilon_u}(u) \cap U$$

és un conjunt finit.

Observació 1.2. *En fer un curs de topologia, s'estén el concepte de boles obertes a un context més general i es defineix un conjunt discret U dins un conjunt K amb una topologia, a un conjunt que compleix que per a cada $u \in U$ té un obert B_u amb $B_u \subset K$ on $B_u \cap U$ és un conjunt finit.*

Observació 1.3. *Molts textos de matemàtica discreta afirmen que discret vol dir un conjunt finit o numerable, però aquest concepte és imprecís com veurem amb exemples si es pensa dins un conjunt ambient amb un valor absolut (o més generalment una topologia). Matemàtica discreta també inclou tot problema relacionat a coomptar i preguntes de comptar objectes dins certes propietats en un conjunt finit, per tant, és una matèria no tipifica on s'inclou molt material molt divers.*

Observació 1.4. *Fixem-nos que en la definició 1.1 podem reemplaçar la condició $B_{\epsilon_u}(u) \cap U$ sigui finit per la condició que compleixi que $B_{\epsilon_u}(u) \cap U$ sigui tant sols l'element u (és dir format per un sol element que correspongui a u). Efectivament, si $B_{\epsilon_u}(u) \cap U = \{u, u_1, \ldots, u_t\}$ és un conjunt finit, com $|u - u_i| = \epsilon_i \leq \epsilon_u$ observem $\epsilon_i \neq 0$ (ja que el valor absolut és zero si i nomes si l'element és zero i $u_i \neq u$), triant $0 < \epsilon'_u$ on $\epsilon'_u < min_{1 \leq i \leq t}(\epsilon_i)$ obtenim que $B_{\epsilon'_u}(u) \cap U = \{u\}$ està format per un sol element.*

1.1.1 Exemples distàncies als racionals

Als nombres racionals hi ha diferents valors absoluts produïnt anàlisis diferents.

1. Denotem per $||_\infty$ el valor absolut usual.
2. Sigui p un nombre primer. Definim :

$$|p^i \frac{n}{m}|_p := p^{-i},$$

on i un enter i n, m enters coprimers amb $mcd(p, nm) = 1$.

Exercici 1.5. *Proveu que $||_p$ defineix un valor absolut no-arquimedià als racionals que anomenem el valor absolut p-adic.*

Lema 1.6. *Si $||$ és un valor absolut no-arquimedià del cos K i $x, y \in K$ amb $|x| \neq |y|$ llavors*

$$|x + y| = maxim(|x|, |y|).$$

Demostració. Suposem $|x| < |y|$. Tenim llavors per la propietat de valor absolut no-arquimedià les desigualtats següents:

$$|y| = |y + x - x| \leq max(|y + x|, | - x|) \leq max(max(|x|, |y|), |x|) = |y|,$$

i per tant hi ha igualtat en totes les inequacions, obtenint $max(|y+x|, |x|) = |y|$ i per tant $|y + x| = |y|$ quan $|y| > |x|$. □

Definició 1.7. *Dos valors absoluts en un cos K són equivalents sempre que $|x|_1 < 1$ es equivalent a $|x|_2 < 1$ per $x \in K$.*

Observació 1.8. És pot demostrar que l'anàlisi (o topologia) donat per dos valors absoluts donen anàlisis (o topologies) diferents en el cos K si i nomes si el dos valors absoluts no són equivalents. Consulteu per exemple [Con23].

Lema 1.9. *Els valors absoluts als nombres racionals $||_\infty$, $||_p$ són no equivalents 2 a 2.*

Demostració. Fixant p primer, i $x = p$ s'obté $|x|_\infty > 1$ i $|x|_p < 1$, i per tant $||_\infty$ és no equivalent a $||_p$ amb p primer. Sigui ℓ un altre primer enter i triem $x = \frac{p}{\ell} \in \mathbb{Q}$, i $|x|_p < 1$ i $|x|_\ell > 1$ on $||_p$ i $||_\ell$ són no-equivalents. □

Fet 1.10 (Ostrowski)**.** *Tot valor absolut als racionals és equivalent a $||_p$ per a cert primer p o bé a $||_\infty$.*

Podeu consultar-ne una demostració (i un aprofundiment en el valors absolut p-àdic) en el llibre [Ko84].

• Anem a fer exemples de conjunts discrets dins els nombres racionals $\mathbb{Q}$. Si S és un conjunt finit dins $\mathbb{Q}$ és sempre un conjunt discret en qualsevol dels valors absoluts als racionals. Què succeeix si S és un conjunt numerable? és sempre discret?

Exemple 1.11. *Sigui p un primer fixat. Considerem*

$$\Omega_p := \{a_n = \frac{1}{p^n}\}_{n\in\mathbb{N}} \cup \{0\} \subset \mathbb{Q}.$$

Fixem-nos que Ω_p és un conjunt numerable.

- *Fixem-nos que Ω_p amb el valor absolut usual $||_\infty$ no és discret perquè té el limit de la successió a_n, i el procés límit usualment no és discret. Efectivament,*

  $$B_\epsilon(0) \cap \Omega_p$$

  és un conjunt no finit perqué $1/p^n <$ epsilon és equivalent a $log_p(\frac{1}{\epsilon}) < n$ i per tant hi ha una infinitud the naturals n complint aquesta última desigualtat un cop ϵ és fixat.

- *Fixem-nos que Ω_p amb el valor absolut p-adic Sí és discret. Anem-ho a demostrar (la idea és que Ω_p no té cap element obtingut via un limit en el valor absolut p-àdic). Tenim $|a_n|_p = p^n$ i $|0|_p = 0$. Clarament $B_1(0) \cap \Omega_p = \{0\}$ és un conjunt finit. Triem $u = 1/p^n$ amb $n \in \mathbb{N}$. Fixem-nos que $1/p^i \notin B_1(1/p^n)$ per $i > n$ (exercici al lector) d'on $\Omega_p \cap B_1(1/p^n)$ és un conjunt finit.*

1.1.2 Valors absoluts en $K[x]$ o $Quot(K[X]) = K(X)$

Si $f \in K[X]$ irreductible i fixant $c > 1$ un nombre real fix, podem definir

$$|f^i(x)\frac{h(x)}{m(x)}|_f := c^{-i}$$

on i enter i $h(x), m(x) \in K[X]$ coprimers amb $mcd(f(x), h(x)m(x)) = (1)$.

Definim també

$$|h(x)/m(x)|_\infty := c^{grau(h(x))-grau(m(x))}$$

Exercici 1.12. *Demostreu que $||_f$ amb $f \in K[X]$ irreductible i $||_\infty$ defineixen valors absoluts en $K(X)$ no equivalents. A més tots aquests valors absoluts són no-arquimedians.*

Qüestió 1.13. *Quina és la completació de $\mathbb{Q}$ respecte el valor absolut $||_\infty$? En algun curs durant el grau hauria de demostrar que correspon al cos dels nombres reals. Quina és la completació de $\mathbb{Q}$ amb el valors absolut p-adics? Quina és la completació de $K[X]$ amb el valor absolut x-àdic?*

Abans de continuar, es convenient llegir aquí la part final d'aquesta subsecció titulada "Nocions sobre la completació d'un cos per un valor absolut" referent a conceptes bàsics de successió de Cauchy i la definició de la completació d'un cos via successions de Cauchy mirant la demostració del Teorema 1.18.

Definició 1.14. *Donat K un cos definim les series formals en la variable X a coeficient en un cos K i s'anota $K[[X]]$ a les expressions en sèrie de poténcies $a(X) := \sum_{n=0}^{\infty} k_n X^n$ amb $k_n \in K$ amb una operació suma coeficient a coeficient i operació producte definida de forma usual on si $b(X) = \sum_{n=0}^{\infty} k'_n X^n$, el grau ℓ de la serie formal $(a(X) \cdot b(X))$ és igual al grau ℓ del polinomi $(\sum_{n=0}^{\ell} k_n X^n)(\sum_{j=0}^{\ell} k'_j X^{j'})$.*

Lema 1.15. *$K[[X]]$ és un anell commutatiu amb $1 \neq 0$.*

Demostració. Exercici al lector. □

Fet 1.16. *La completació de $K[X]$ amb el valor absolut x-àdic és $K[[X]]$.*

Definim un morfisme epimorfisme entre les successions de Cauchy de $K[X]$ a $K[[X]]$,

Demostració. Aquest curs sol demostrem que tot element de $K[[X]]$ es pot pensar com una successió de Cauchy de $K[X]$.

Considera $a(X) := \sum_{n=0}^{\infty} k_n X^n \in K[[X]]$ i considerem la successió en $K[X]$: $((a_n := \sum_{t=0}^{n} k_t X^t))_n$.

Fixem-nos que $|a_{n+m} - a_n|_X = |\sum_{t=n+1}^{n+m} k_t X^t|_X \leq max_{n+1 \leq t \leq n+m}(|k_t X^t|_X) \leq |X^{n+1}|_X = c^{-n-1}$ i per tant és una successió de Cauchy i per tant en la completació té sentit fer-hi limit a la successió que correspon a la sèrie formal $a(X)$. Per detall com la successió de Cauchy correspon a un element del cos completat cal entendre la demostració d'aquests apunts del Teorema 1.18 □

Nocions sobre la completació d'un cos per un valor absolut

Denotem per $(K, ||)$ un cos K amb un valor absolut $||$.

Una successió $\{a_n\}_{n \geq 0}$ una successió d'elements en K, diem que és de Cauchy si $\forall \epsilon > 0$, $\exists n_0(\epsilon)$ on $\forall m \geq n \geq n_0(\epsilon)$ es té $|a_m - a_n| < \epsilon$.

Una successió es diu que és convergent de límit $a \in K$ si $\forall \epsilon > 0$ $\exists n_0(\epsilon)$ on $\forall n \geq n_0(\epsilon)$ es satisfà $|a_n - a| < \epsilon$.

(És fàcil observat que tota successió convergent és de Cauchy, i que tota successió de Cauchy és fitada).

Definició 1.17. *Un cos $(K, ||)$ és complet quant tota succesió de Cauchy d'elements de K convergeix a un element de K.*

Teorema 1.18. *Donat $(K, ||_K)$. Existeix un cos $\hat{K}$ i un valor absolut $||_{\hat{K}}$ complint,*

1. *$(\hat{K}, ||_{\hat{K}})$ és un cos complex amb $||_{\hat{K}}$,*

2. *$K \subset \hat{K}$ i $||_{\hat{K}} : K \to \mathbb{R}_{>0}$ coincideix amb $||_K$,*

3. *K és dens en $\hat{K}$.*

4. *Si $(\hat{K}_1, ||_1)$, $(\hat{K}_2, ||_2)$ són dos cossos que satisfan les propietats anteriors, aleshores existeix un morfisme de cossos únics $\varphi : \hat{K}_1 \to \hat{K}_2$ amb $\varphi_{|_K} = id$ amb $|\varphi(x)|_2 = |x|_1$.*

La parella $(\hat{K}, ||_{\hat{K}})$ s'anomena una completació de $(K, ||)$ i és única llevat isometria de cossos per l'última propietat.

Demostració. Considera $\mathcal{C}(K)$ el conjunt de successions de Cauchy en el cos K. Observem donats $(a_n)_n, (b_n)_n \in \mathcal{C}(K)$, tenim definides les operacions:

$$(a_n)_n + (b_n)_n := (a_n + b_n)_n \in \mathcal{C}(K),$$

$$(a_n)_n * (b_n)_n := (a_n b_n)_n \in \mathcal{C}(K),$$

que doten $\mathcal{C}(K)$ d'anell commutatiu amb unitat.

Fixem-nos que $K \subset \mathcal{C}(K)$ via donat $k \mapsto (k)_n$ a la successió de Cauchy(i convergent) constant igual a k per tot $n \in \mathbb{N}$.

Denotem per $\mathfrak{M}$ el conjunt de les successions convergents de límit $0 \in K$. Clarament $\mathfrak{M}$ és un ideal de $\mathcal{C}(K)$ (la suma de dos successions convergents a zero és convergent a zero, i el producte d'una successió de Cauchy amb una convergent a zero és una successió convergent a zero). Fixem-nos que $\mathfrak{M}$ és un ideal maximal de $\mathcal{C}(K)$ ja que si $c = (c_n)_n \in \mathcal{C}(K) \setminus \mathfrak{M}$, fixem-nos llavors que per $n \geq n_0$ un natural fix $c_n \neq 0$ (ja que no és convergent a zero) i la successió $(\frac{1}{c_n})_{n \geq n_0}$ és fàcil veure que és una successió de Cauchy i per tant $(c_n)_n \in \mathcal{C}(K)^*$ i es pot demostrar que llavors$\mathcal{C}(K)/\mathfrak{M}$ és domini commutatiu i per l'anterior tot element no zero té un invers i per tant és un cos.

Escrivim $\hat{K} := \mathcal{C}(K)/\mathfrak{M}$ el cos que per construcció $K \subset \hat{K}$ on $k \mapsto [(k)_n]$, que és injectiva.

Definim $||_{\hat{K}}$, donat $(x_n)_n \in \mathcal{C}(K)$, via

$$|(x_n)_n|_{\hat{K}} := \lim_{n \to \infty} |x_n|_K \in \mathbb{R},$$

on observem que té sentit ja que la successió de nombres reals $(|x_n|)_n$ és de Cauchy i per tant convergent (efectivament, com $(x_n)_n$ de Cauchy en K, tenim $\forall \epsilon > 0$ $\exists n_0(\epsilon)$ complint $|x_m - x_{n_0(\epsilon)}| < \epsilon$, on $|x_m| \leq |x_m - x_{n_0(\epsilon)}| + |x_{n_0(\epsilon)}| < \epsilon + |x_{n_0(\epsilon)}|$, d'aquí $|x_m| - |x_{n_0(\epsilon)}| < \epsilon$).

Llavors la tupla $(\hat{K}, ||_{\hat{K}})$ és el cos complet que satisfà les condicions demanades. Exercici al lector.

Demostrem tan sols aquí que $\hat{K}$ és complet amb $||_{\hat{K}}$.

Considerem $(d_n)_n \in \mathcal{C}(\hat{K})$ una successió de Cauchy en $(\hat{K}, ||_{\hat{K}})$. Escrivim $d_m = [(a_{i,m})_i] \in \mathcal{C}(K)$. Fixem-nos que $\forall \epsilon > 0$ i $\forall n, m \geq n_0(\epsilon)$ tenim

$$|d_n - d_m|_{\hat{K}} = \lim_{i \to \infty} |a_{i,n} - a_{i,m}| < \epsilon.$$

Triem $\alpha = [(\alpha_i)_i]$ la successió definida per $\alpha_i := a_{i,n_0(1/10^i)}$ pensant que triem successió creixent de naturals amb $n_0(1/10^i) < n_0(1/10^{i+1})$ (amb límit $+\infty$). És fàcil demostrar que $\alpha \in \hat{K}$. Observeu finalment que donat $\epsilon' > 0$ existeix i on $\epsilon' > \frac{1}{10^i}$ i per tant per $n \geq n_0(1/10^i)$ tenim que $|d_n - \alpha|_{\hat{K}} = \lim_{i \to \infty} |a_{i,n} - a_{i,n_0(1/10^i)}| < \frac{1}{10^i} < \epsilon'$ $\forall n \geq n_0(1/10^i)$ obtenint $(d_n)_n$ convergeix en $\alpha \in \hat{K}$. $\square$

Tenim el següent resultat que no demostrarem en aquest curs,

Teorema 1.19 (Ostrowski)**.** *Sigui K cos complet respecte d'un valor absolut arquimedià $||$. Llavors $(K, ||)$ és isomorf (una isometria) a $(\mathbb{R}, ||_\infty)$ ó $(\mathbb{C}, ||_\infty)$.*

1.2 Conjunts discrets dins espai vectorial $\mathbb{R}^N$: Xarxes

Definició 1.20. *Sigui $V = \{v_1, \ldots, v_k\}$ un conjunt de $1 \leq k (\leq N)$ vectors linealment independents de $\mathbb{R}^N$. El conjunt*

$$\Lambda(V) := \{\sum_{k=1}^{k} n_i v_i | n_i \in \mathbb{Z}\}$$

s'anomena una xarxa de $\mathbb{R}^N$ amb base $(v_1, \ldots, v_k)$ de mida k. Si $k = N$ diem que és una xarxa de $\mathbb{R}^N$ de mida màxima.

Definició 1.21. *Considerem V un K-espai vectorial amb una norma (o mètrica) $\|\|$ (concepte donat durant el curs d'Àlgebra Lineal). Donat $v \in V$ podem considerar la bola centrada en v i radi ϵ al subconjunt de V següent:*

$$B_\epsilon(u) = \{v \in V | \|v - u\| < \epsilon.$$

Diem que un subconjunt $U \subset V$ és discret respecte la norma en V si per a tot $u \in U$ existeix un real positiu ϵ_u on

$$B_{\epsilon_u}(u) \cap U$$

és un conjunt finit.

En aquesta subsecció pensarem $V = \mathbb{R}^N$ com $\mathbb{R}$-espai vectorial amb la norma euclidiana en V.

Lema 1.22. *El conjunt $\Lambda(V)$ és un grup abelià i amb la norma euclidiana de $\mathbb{R}^N$ és un conjunt discret de $\mathbb{R}^N$.*

Demostració. Exercici al lector. □

Fixem-nos que si escrivim $v_i = \begin{pmatrix} v_{1,i} \\ \vdots \\ v_{N,i} \end{pmatrix} \in \mathbb{R}^N$ com vectors columna podem escriure

$$\Lambda(V) = \{\begin{pmatrix} v_{1,1} & \ldots & v_{1,k} \\ \vdots & \ddots & \vdots \\ v_{N,1} & \ldots & v_{N,k} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix} | x = \begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix} \in \mathbb{Z}^k\}$$

on $\mathbb{Z}^k$ amb k enter denota també $M_{k,1}(\mathbb{Z})$, i el context fa entenedor quan ens referim a element fila o element columna per al producte cartesià de $\mathbb{Z}$ amb ell mateix k cops.

Observació 1.23. *Considerem $V' := \{v_1, \dots, v_\ell\} \subset \mathbb{R}^N$ però on els vectors $v_1, \dots, v_\ell$ NO són linealment independents. Podriem també escriure*

$$\tilde{\Lambda}(V') := \{(v_1|\dots|v_\ell) \cdot x | x \in \mathbb{Z}^\ell)\} \subset \mathbb{R}^N.$$

No obstant ara no necessàriament aquest conjunt és discret amb l'anàlisi en $\mathbb{R}^N$ de la norma euclidiana que feu en un curs d'anàlisi real en la titulació.

Exemple 1.24. *Considera $V' = \{1, \sqrt{2}\} \subseteq \mathbb{R}$ i considerem*

$$\tilde{\Lambda}(V') = \{n_1 \cdot 1 + n_2\sqrt{2} | n_i \in \mathbb{Z}\}$$

no és discret amb el valor absolut $||_\infty$ pel lema d'aproximació següent.

Lema 1.25. *(d'aproximació) Sigui θ un nombre irracional i $q > 1$ un enters. Llavors existeixen x, y enters complint*

$$|y - x\theta| < \frac{1}{q} (\leq \frac{1}{x})$$

amb $0 < x \leq q$, on el valor absolut és el valor absolut arquimedià usual en els nombres reals.

Demostració. Fent $x_i \in \{0, \dots, q\} \subset \mathbb{N}$, per cada x_i triem y_i enter amb $0 \leq y_i - x_i\theta < 1$. Tenim $q+1$ valors de $Y - X\theta$ en els q-intervals

$$[\frac{r}{q}, \frac{r+1}{q}),\ r = 0, \dots, q-1.$$

Per tant hi ha dos valors de $y_i - x_i\theta$ dins el mateix interval, sense pèrdua de generalitat podem pensar que els dos valors corresponen a $i = 1, 2$ i per tant,

$$|(y_1 - y_2) - (x_1 - x_2)\theta| < \frac{1}{q} \leq \frac{1}{x_1 - x_2}.$$

□

Corol·lari 1.26. *Donat θ un nombre irracional, llavors hi ha una infinitut de solucions a $\mathbb{Z}$ de la inequació*

$$|Y - X\theta| < 1/X.$$

Demostració. Pel lema d'aproximació tenim que l'anterior inequació té una solució a $\mathbb{Z}$. Escrivim-la via $|\alpha_1 - \beta_1\theta| < 1/\beta_1$. Triant $q_1 > \frac{1}{|\alpha_1 - \beta_1\theta|}$, usant el lema anterior podem obtenir una solució diferent complint $|\alpha_2 - \beta_2\theta| < 1/q_1 \leq \frac{1}{\beta_2}$,[1] e iterant el procés triant $q_i > \frac{1}{|\alpha_i - \beta_i\theta|}$ construïm solució $(\alpha_{i+1}, \beta_{i+1})$ satisfent la inequació diferent de les anteriors usant el lema anterior, per $i \geq 1$ enter. □

Demostració. Detallem per alguns alumnes perquè $\tilde{\Lambda}(1, \sqrt{2})$ no és un conjunt discret dins $\mathbb{R}$. Com vaig comentar és obvi a partir de la demostració del Corol.lari anterior, efectivament: fixem $\epsilon > 0$ i volem demostra que $B_\epsilon(0) \cap \tilde{\Lambda}(1, \sqrt{2})$ no és finit mai. Triem $q = q_0$ enter on $\frac{1}{q} < \epsilon$, llavors pel lema

[1] fixem-nos que $|\alpha_1 - \beta_1\theta| > 1/q_1$ per la tria de q_1 i per tant com el valor absolut és diferent $\alpha_1 - \beta_1\theta$ és diferent a $\alpha_2 - \beta_2\theta$

d'aproximació tenim una solució $|\alpha_1+\sqrt{2}\beta_1| < 1/q < \epsilon$ amb $\alpha_1, \beta_1 \in \mathbb{Z}$. Seguint la demostració del Corol.lari anterior anem construïnt α_n, β_n amb $\alpha_n + \beta_n\sqrt{2}$ tots diferents amb $|\alpha_n + \beta_n\sqrt{2}| < 1/q_{i-1} < 1/q < \epsilon$ i per tant $B_\epsilon(0) \cap \tilde{\Lambda}(1, \sqrt{2})$ no és finit. □

Observació 1.27. **[Notació]** Donada una matriu $B \in M_{N,M}(\mathbb{R})$ denotem per $\Lambda(B) := \{B \cdot z | z \in \mathbb{Z}^M\} \subseteq \mathbb{R}^N$ si $rang(B) = M$ i $\tilde{\Lambda}(B) := \{B \cdot z | z \in \mathbb{Z}^M\} \subseteq \mathbb{R}^N$ en general.

Definició 1.28. *Una matriu U quadrada a coeficients enters ($U \in M_N(\mathbb{Z})$) s'anomena unimodular si $|det(U)|_\infty = 1$.*

Exercici 1.29.

- *Demostreu que el producte de $k \geq 1$ matrius unimodulars de mida N és també una matriu unimodular de mida N.*
- *Demostreu que $U \in M_N(\mathbb{Z})$ és unimodular si i només si U té matriu inversa i aquesta matriu inversa pertany a $M_N(\mathbb{Z})$. En particular la inversa d'una matriu unimodular és unimodular.*
- *Demostreu que si $U \in M_N(\mathbb{Z})$ és unimodular llavors: $x \in \mathbb{Z}^N \Leftrightarrow U \cdot x \in \mathbb{Z}^N$.*

Lema 1.30. *Sigui $B, B' \in M_{N\times M}(\mathbb{R})$.*

1. *Si $B = B' \cdot U$ amb U unimodular llavors $\tilde{\Lambda}(B) = \tilde{\Lambda}(B')$.*
2. *Si $rang(B) = rang(B') = M$ i $\Lambda(B) = \Lambda(B')$ llavors existeix una matriu U unimodular on $B = B' \cdot U$.*

Demostració.

1. Si $y \in \tilde{\Lambda}(B)$ tenim existeix $x \in \mathbb{Z}^M$ on $y = B \cdot x = B'(Ux)$ ara per l'exercici 1.29 $Ux \in \mathbb{Z}^M$ i per tant $y \in \tilde{\Lambda}(B')$. L'altra inclusió és similar usant que U^{-1} és una matriu unimodular, exercici al lector.

2. Suposem $\Lambda(B) = \Lambda(B')$ i escrivim $B = (b_1|\dots|b_M)$ on b_i vectors columna de $\mathbb{R}^N$. Com cada $b_i \in \Lambda(B')$ existeix $x_i \in \mathbb{Z}^M$ complint

$$b_i = B'(x_i)$$

i per tant $B = B' \cdot V$ on $V \in M_M(\mathbb{Z})$ on $V = (x_1|\dots|x_M)$. Amb un argument similar obtenim $B' = B \cdot W$ amb $W \in M_N(\mathbb{Z})$. D'on obtenim les igualtats

$$B' = B' \cdot (V \cdot W); \ \ , B = B \cdot (W \cdot V).$$

Ara com $rang(B) = rang(B') = M$, no hi ha cap combinació lineal entre les columnes de B o B' per tant $V \cdot W = I_M = W \cdot V$, i per tant V i W són matrius unimodulars (ja que ambdues tenen coeficients enters, una és inversa de l'altra i com el determinant de la inversa és invers del determinant de l'altra obtenim que el seu determinant és ± 1). [2]

□

[2] Detallo com de la igualtat $B = B(WV)$ amb $rang(B) = M$ podem concloure que $WV = I_M$. Claramenet de la igualtat obtenim $B(I_M - VW) = (0)$ on (0) denota la matriu MxM de tot zeros. Ara si fixem C_i la columna i-essima de $I_M - VW$ en fer BC_i és la columna i de (0) i per tant tot de zeros, obtenint una combinació lineal de les columnes de B igual a la columna zero, ara com el $rang(B) = M$ l'única combinació lineal és que tot sigui zeros per tant la columna C_i és la columna tot de zeros.

Definició 1.31. *Siguin Λ, Λ' dues xarxes de $\mathbb{R}^N$ ambdues de mida M. Si $\Lambda' \subseteq \Lambda$ diem que Λ' és una subxarxa de Λ.*

Observació 1.32. *El Lema anterior 1.30 afirma que la base per a qualsevol xarxa Λ és pot variar via multiplicar per la dreta per una matriu unimodular.*

Qüestió 1.33. *Hi ha una manera de triar bases amb certa relació d'unicitat entre una xarxa i una subxarxa? Veieu Teorema 1.47*

Observació 1.34. *Si $\Lambda = \Lambda(B)$ una xarxa de dimensió màxima en $\mathbb{R}^N$, observeu que $|det(B)|_\infty$ és independent de l'elecció de B pel lema anteior i aquest real s'anomena el determinant de la xarxa Λ: $det(\Lambda) := |det(B)|_\infty$.*

1.3 Transformacions elementals unimodulars. Resolució entera de sistemes lineals

Diem que hi ha tres transformacions elementals unimodulars per a una matriu $B \in M_{N,M}(K)$ on $\mathbb{Z} \subset K$:

- Intercanviar 2 files o dues columnes de la matriu,
- multiplicar una fila o una columna per -1,
- Sumar a una fila un múltiple ENTER d'una altra fila,
  Sumar a una columna una múltiple ENTER d'una altra columna.

Observació 1.35. Fixem-nos, relacionant-ho amb el curs d'Àlgebra Lineal de primer curs, que les transformacions elementals anteriors corresponen a matrius elementals que són matrius unimodulars, i per tant, donada $B \in M_{N,M}(K)$ e iterant diferents canvis elementals en files i columnes obtenim una nova matriu que correspon a una matriu $U \cdot B \cdot V$ amb U, V matrius unimodulars (on U prové del producte en ordre de matrius elementals unimodulars corresponent a les transformacions en files que realitzem, i V prové del producte amb ordre de les diferentes transformacions en columnes que hem anat realitzant).

Recordem que $diag(a_1, a_2, \ldots) = D \in M_{N,M}(K)$ denota la matriu on els valors no zero corresponen a la diagonal i la el valor en la fila i columna i de D correspon a a_i.

Definició 1.36 (forma normal d'Smith)**.** *Sigui $B \in M_{N\times M}(\mathbb{Z})$ si existeixen matrius U,V unimodulars on*

$$U \cdot B \cdot V = diag(n_1, \ldots, n_d, 0, \ldots, 0) \in M_{N\times M}(\mathbb{Z})$$

amb n_i naturals on $n_i | n_{i+1}$ per a $i = 1, \ldots, d-1$. Diem que $diag(n_1, \ldots, n_d, 0, \ldots, 0) \in M_{N\times M}(\mathbb{Z})$ és una forma normal d'Smith associada a la matriu B.

Observació 1.37. *Observeu que un anàleg d'una forma normal d'Smith dins un curs d'Àlgebra Lineal amb operacions elementals en un cos enlloc d'un anell com $\mathbb{Z}$ està relacionat amb la PAQ-reducció.*

Definició 1.38 (forma normal d'Hermite)**.** *Donat $B \in M_{N\times M}(\mathbb{Z})$ de rang M diem que té forma normal en files d'Hermite H si existeix una matriu unimodular U on $H = U \cdot B$ on H compleix les condicions següents:*

1. *H és una matriu triangular superior (i.e. $h_{i,j} = 0$ per a $i > j$) i totes les files de zero es troben abaix de tot.*

2. *Es compleix $0 \leq h_{i,j} < h_{j,j}$ per a $i < j$*

Una matriu H complint les dues condicions anteriors s'anomona una matriu d'Hermite.

Hi ha una definicó anàloga pel cas de forma normal d'Hermite en columnes, transposant la definició anterior (exercici al lector).

Teorema 1.39. *Existeix una forma nomal d'Smith associada a $B \in M_{N\times M}(\mathbb{Z})$.*

Demostració. És suficient demostrar que tota matriu no trivial hi ha operacions elementals unimodulars en files i columnes sobre la matriu B (i per tant multiplicant per certes matrius unimodulars U_1, V_1, i $B_1 = U_1 \cdot B \cdot V_1$) per a obtenir

$$B_1 = \left(\begin{array}{c|ccc} f_1 & 0 & \dots & 0 \\ \hline 0 & & & \\ \vdots & & C_1 & \\ 0 & & & \end{array}\right);$$

amb $f_1 > 0$ natural i $C_1 \in M_{N-1\times M-1}(\mathbb{Z})$ on f_1 divideix a cada coeficient de C_1, on iterant el procediment fins arribar a que C_i és la matriu de zero o no queda matriu, s'obté una forma normal Smith associada a B.

Explicitem ara un algoritme iteratiu fent canvis unimodulars elementals en files i columnes a B per a obtenir B_1, escrivim $B = (b_{i,j})_{i,j}$ on $b_{i,j}$ coeficient en la matriu B corresponent a la fila i i columna j de la matriu B.

Algorisme:
Pas inici, matriu B.

- Cas 1. En la fila 1 ha ha $b_{1,j}$ on $b_{1,1} \nmid b_{1,j}$. Llavors per l'algorisme d'Euclides
$$b_{1,j} = b_{1,1}q + b$$
amb $0 < b \leq |b_{1,1}|$. Fem $C_{j,Nova} := C_j - qC_1$ (a la columna j li restem q cops la columna 1) e intercanviem columna 1 amb columna j. I tornem amb la matriu resultat al pas inici.

- Cas 2. (En el cas que cas 1 no es dóna), en la columna 1 hi ha $b_{j,1}$ on $b_{1,1} \nmid b_{j,1}$, fem un procediment anàleg al realitzat en el cas 1 (però en files enlloc de columnes) per a obtenir el nou $b_{1,1}$ amb valor absolut més petit que el que teniem, i a més positiu. I tornem amb la matriu resultat al pas inici com a nova matriu B d'inici.

- Cas 3. (En el cas 1 i 2 no es donen). Si $b_{1,1}$ divideix cada element de la fila 1 i columna 1, fent operació elemental tercera fem zeros amb canvis

elementals unimodulars a sota i a la dreta del $b_{1,1}$ i obtenim una matriu de la forma

$$prova(B_1) = \left(\begin{array}{c|ccc} b_{1,1} & 0 & \dots & 0 \\ \hline 0 & & & \\ \vdots & & C_1' & \\ 0 & & & \end{array}\right);$$

Si $b_{1,1}$ divideix cada element de C_1' ja hem finalitzat i $prova(B_1)$ triem com matriu B_1. En cas que no $\exists$ un coeficient de C_1', diem $c_{i+1,j+1}$ (corresponent a la fila i,columna j de C_1') on $b_{1,1} \nmid c_{i+1,j+1}$ fem $F_{1,nova} = F_1 + F_{i+1}$, és dir sumem la fila $i+1$ a la fila 1 de la matriu B. I tornem amb la matriu resultat al pas inici.

I tornem amb la matriu resultant al pas inici.

Aquest pas 1,2, i 3 finalitza algun moment, ja que 1,2 sempre redueix coeficient $|b_{1,1}|$ i el pas 3 un cop fet els pas 1 o 2, també, com nombres naturals menors que un de fix és un nombre finit, aquest procediment finalitza en algún moment.

Un cop obtinguda B_1, iterem el procediment fins a obtenir una forma d'Smith. □

El següent resultat es demostrarà a la classe de problemes del curs.

Fet 1.40. *Donada $B \in M_{N\times M}(\mathbb{Z})$, sol hi ha una única forma normal d'Smith associada a B i que denotarem per $Sm(B)$.*

Corol·lari 1.41. *Tota matriu unimodular $\tilde{U}$ de mida N és producte de matrius elementals unimodulars, i per tant tota matriu unimodular s'obté com a producte de matrius elementals unimodulars.*

Proof. De la demostració de l'existència de la forma normal Smidth per a $B = \tilde{U}$ tenim existeixen U, V unimodulars que provenen de producte de matrius elementals unimodulars on $U\tilde{U}V = diag(n_1, \dots, n_N) = Sm(B)$. Ara com el determinant de $Sm(B)$ ha de ser ± 1 això implica que $n_1, \dots, n_N = 1$ i com la inversa d'una matriu unimodular elemental és també una matriu unimodular elemental obtenim $\tilde{U}$ és producte de matrius unimodulars elementals (ja que U i V son producte de matrius elementals unimodulars i també ho compleix U^{-1} i V^{-1} i per tant també és producte de matrius elementals $U^1V^{-1} = \tilde{U}$). □

Observació 1.42. *Magma té implementat com donada $B \in M_{N\times M}(\mathbb{Z})$ trobar la forma normal d'Smith $Sm(B)$ associada a B i unes matrius unimodulars U, V on $U \cdot B \cdot V = Sm(B)$, via el codi Magma següent:*

```
INPUT:\\
B:=Matrix(3,4,[2,3,6,2,5,6,1,6,8,3,1,1]);
B;
Sm,U,V:=SmithForm(B);
Sm;
U;
V;
U*B*V;
OUTPUT:
```

```
[2 3 6 2]
[5 6 1 6]
[8 3 1 1]
[1 0 0 0]
[0 1 0 0]
[0 0 1 0]
[1 0 0]
[0 1 0]
[0 0 1]
[ -31   13  -16  -63]
[ 119  -50   62  242]
[ -19    8  -10  -39]
[ -90   38  -47 -183]
[1 0 0 0]
[0 1 0 0]
[0 0 1 0]
```

Podeu introduir el codi a : `http://magma.maths.usyd.edu.au/calc/`

Lema 1.43. *Donat un sistema lineal de M equacions i N incògnites a coeficients enters $(B|b)$ i matrius U, V unimodulars on $Sm(B) = U \cdot B \cdot V$. Llavors les solucions $(x_1, \ldots, x_N) \in \mathbb{Z}^N$ del sistema lineal, corresponen a*

$$\begin{pmatrix} x_1 \\ \vdots \\ x_N \end{pmatrix} = V \begin{pmatrix} y_1 \\ \vdots \\ y_N \end{pmatrix}$$

on $(y_1, \ldots, y_N) \in \mathbb{Z}^N$ són les solucions enteres de $Sm(B) \begin{pmatrix} y_1 \\ \vdots \\ y_N \end{pmatrix} = U \cdot b$.

Demostració. Observeu que $(B|b) = (U^{-1}Sm(B)V^{-1}|b)$ i per tant son equivalents a les solucions enteres de $(Sm(B)V^{-1}|U \cdot b)$. Ara fent el canvi de variables $y = V^{-1}x$ obtenim el resultat. □

Exemple 1.44. *Trobeu les solucions enteres pel sistema lineal*

$$\left(\begin{array}{cccc|c} 2 & 3 & 6 & 2 & 2 \\ 5 & 6 & 1 & 6 & -1 \\ 8 & 3 & 1 & 1 & 3 \end{array}\right).$$

Tenim que hem calculat abans la foma Smith i matrius unimodulars on $U = I_3$ i obtenim sistema en $(y_1, \ldots, y_4)$ a estudiar següent:

$$\left(\begin{array}{cccc|c} 1 & 0 & 0 & 0 & 2 \\ 0 & 1 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 & 3 \end{array}\right),$$

d'on $(y_1, y_2, y_3, y_4) = (2, -1, 3, t)$ amb $t \in \mathbb{Z}$ i per tant

$$\begin{pmatrix} x_1 \\ \vdots \\ x_N \end{pmatrix} = \begin{pmatrix} -31 & 13 & -16 & -63 \\ 119 & -50 & 62 & 242 \\ -19 & 8 & -10 & -39 \\ -90 & 38 & -47 & -183 \end{pmatrix} \begin{pmatrix} 2 \\ -1 \\ 3 \\ t \end{pmatrix} = \begin{pmatrix} -123 - 63t \\ 474 + 242t \\ -76 - 39t \\ -359 - 183t \end{pmatrix}.$$

Teorema 1.45. *Donada $E \in M_{N\times M}(\mathbb{Z})$ amb rang M, existeix una forma normal d'Hermite en files H associada a E i matriu unimodular U on $U\cdot E = H$.*

Demostració. [Un esboç] Un algorisme és el següent, on $B_k = \left(\begin{array}{c|c} H_k & C_k \\ \hline 0 & D_k \end{array}\right)$ on H_k és una matriu $k \times k$ en forma normal d'Hermite en files, i s'obté B_{k+1} a partir de B_k de la forma algorítmica següent:

Sigui $d_1, \ldots, d_{n-k}$ les entrades en la primera columna de D_k, podem pensar tots > 0 (multiplicant la fila corresponent per -1 si fa falta). Escrivim $d = gcd(d_1, \ldots, d_{n-k})$ per a posar-ho al coeficient $k+1, k+1$ de la matriu usant el Pas 1, Pas 2 de la demostració del Teorema 1.39 fent operacions unimodulars tant sols en files involucrant les files $k+1$ fins n, tot fent zeros a sota posició $k+1, k+1$ un cop aconseguit el valor d en aquesta posició via tercera operació elemental unimodular, i també sobre de la posició $k+1, k+1$ fent que els enters sobre aquest pivot de valor d siguintots positius o zero i menors que d. □

Observació 1.46. Hi ha un anàleg per a forma normal d'Hermite en columnes, que la formulació del resultat anàleg al Teorema anterior és:
Donada $E \in M_{N,M}(\mathbb{Z})$ de rang N, llavors existeix una forma normal d'Hermite en columnes H i U unimodular complint que $EU = H$.

Teorema 1.47. *Sigui $\Lambda' \subset \Lambda \subset \mathbb{R}^N$ on Λ' és una subxarxa de Λ, i Λ i Λ' són de dimensió màxima N. Llavors per a cada base $(b_1, \ldots, b_N)$ de Λ on $\Lambda(B = (b_1|\ldots|b_N))$ existeix una base $(b'_1|\ldots|b'_N)$ de $\Lambda' = \Lambda(B' = (b'_1|\ldots|b'_N))$ on $B' = B \cdot H$ on H és una matriu en forma normal d'Hermite en columnes.*

Demostració. Com $\Lambda' \subset \Lambda(B)$ tenim que $B' = B \cdot V$ amb V una matriu a coeficients enters. Per tant existeix U unimodular complint que $VU = H$ (amb H en forma normal d'Hermite en columnes) d'aquí

$$B' \cdot U = B \cdot V \cdot U = B \cdot H$$

Ara les columnes de $B' \cdot U$ continua donant una base per a Λ' pel Lemma 1.30, per tant el resultat. □

Observació 1.48. *Magma pot calcular també una forma normal d'Hermite en files via la instrucció*

```
H,U:=HermiteForm(V);
```

1.4 Classificació de grups abelians finit generats

Definició 1.49. *Un grup abelià F s'anomena lliure en un subconjunt $A \subset F$ si per a tot $x \in F$ amb $x \neq 0$, existeixen enters únics $n_1, \ldots, n_r \in \mathbb{Z}$ i elements únics d'A: $a_1, \ldots, a_r \in A$ complint que $x = n_1a_1 + \ldots + n_ra_r$. Diem llavors que A forma una base per a F.*

Observació 1.50. Si F és un grup abelià lliure, llavors element neutre 0_F de F sempre s'escriu per a tot subconjunt finit A' de A com $0_F = m_1a'_1 + \ldots m_ta'_t$ amb $A' = \{a'_1, \ldots, a'_m\}$ i m_i naturals tots iguals a zero. Efectivament, si no

fos així voldria dir existeix un conjunt finit A' i $m_i's$ no tots zeros i per tant un $x \neq 0_F$ tindriem que x i $x + O_F = x$ tindrien dos expressions, en contra la definició de grup abelià lliure.

Observació 1.51. Fixem-nos que si F és un grup abelià lliure on 0_F és l'element neutre, llavors F no té torsió.

Efectivament, recordem que un $f \in F$ amb $f \neq 0_F$ és de torsió si existeix un natural $n \neq 0$ on $nf = 0_F$, com $f = n_1a_1 + \ldots + n_ra_r$ amb $a_i \in F$ únics i n_i's naturals únics i no són tots zeros perquè $f \neq 0_F$ tenim $n \cdot f = (nn_1)a_1 + \ldots + (nn_r)a_r$ i per la unicitat de l'expressió no potser igual al neutre.

Lema 1.52. *Si $\mathcal{B}_1, \mathcal{B}_2$ són dues bases per un grup abelià lliure F llavors tenen la mateixa cardinalitat.*

Demostració. En aquest curs sol demostrarem pel cas que ambdues bases $\mathcal{B}_i$ son finites. Observem que si $\mathcal{B} = \{v_1, \ldots, v_t\}$ una base de F formada per un número finit d'elements (tenim que podem escriure $F = \mathbb{Z}v_1 + \ldots + \mathbb{Z}v_t$ i les expressions amb aquesta suma són úniques).

Considerem $2F$, que és un subgrup (abelià) de F (exercici al lector) i en particular es subgrup normal de F d'aquí obtemin que $F/2F$ és un grup abeliá on compleix $[x] + [x] = [0_F]$ i això permet dotar a $F/2F$ d'espai vectorial sobre el cos $K = \mathbb{F}_2$ (exercici al lector).

Provem tot seguit que $\{[v_1], \ldots, [v_t]\}$ és una base del $\mathbb{F}_2$-espai vectorial $F/2F$: *clarament és un sistema generador perquè donat $[x] \in F/2F$ podem escriure $x = n_1v_1 + \ldots + n_tv_t$ amb n_i's natural i per la propietat del grup quocient tenim

$$[x] = n_1[v_1] + \ldots + n_t[v_t]$$

i com $2[v_i] = [0_F]$ tenim $[x] = \tilde{n_1}[v_1] + \ldots + \tilde{n_t}[v_t]$ on $\tilde{n_i}$ és la reducció mòdul 2, on $\tilde{n_i} \in \mathbb{F}_2$.

*per a demostrar que $[v_1], \ldots, [v_t]$ son $\mathbb{F}_2$-linealment independents, observem que si no ho fossin tenim una igualtat en $F/2F$ de la forma

$$[v_{i_1}] + \ldots + [v_{i_k}] = [0_F]$$

on $\{v_{i_1}, \ldots, v_{i_k}\}$ un subconjunt de la base $\mathcal{B}$ i per tant en F tenim

$$v_{i_1} + \ldots + v_{i_k} = 2k_1v_1 + \ldots + 2k_tv_t$$

per a certs k_i's enters, cosa imposible de ser F lliure, per tant obtenim que $[v_1], \ldots, [v_t]$ son vectors $\mathbb{F}_2$-linealment independents de $F/2F$.

Tornem ara a la demostració del Lemma. Si tenim dues bases $\mathcal{B}_i$, ambdues finites d'ordres Ω_i respectivament, obtenim que

$$dim_{\mathbb{F}_2} F/2F = \Omega_i$$

i per tant $\Omega_1 = \Omega_2$ com volíem demostrar. □

Definició 1.53. *Donat F un grup abelià lliure amb una base A, llavors el rang del grup abelià lliure correspon al cardinal del conjunt A.*

Exemple 1.54. *El grup abelià $(\mathbb{Z}^\ell, +)$ és pot demostrar (exercici al lector) que és un grup lliure de rang ℓ on una base és:* $(1, 0, \ldots, 0), \ldots, (0, \ldots, 0, 1)$.

Teorema 1.55. *Sigui M un grup abelià lliure de rang $\ell \in \mathbb{N}$. Llavors qualsevol subgrup N de M és lliure de rang com a molt ℓ.*

Demostració. Fem-ho per inducció respecte del rang ℓ del grup abelià M.

Suposem que $\ell = 1$. Llavors $\varphi : M \cong \mathbb{Z}$ un isomorfisme de grups abelians (fem anar una base $\{e_1\}$ de M via $e_1 \mapsto 1$). Com N és un subgrup de M, correspon $\varphi(N)$ a un ideal $n\mathbb{Z}$ de $\mathbb{Z}$, si $n = 0$, tenim $N = 0$ de ser φ mono i N és lliure de rang zero. Suposem $n \neq 0$. Podem construir $\psi : \mathbb{Z} \to N$ via $m \mapsto m\varphi^{(-1)}(n)$ que és un morfisme de grups epi i mono (exercici al lector), per tant $N \cong \mathbb{Z}$ i per tant N és un grup abelià lliure amb base l'element $\varphi^{-1}(n) \in N$ i per tant de rang 1.

Suposem ara el teorema cert per a grups abelians lliures fins a rang $\ell - 1$. Sigui $x_1, \ldots, x_\ell$ una base per a un grup abelià lliure M de rang ℓ i volem demostrar que tot subgrup és lliure de rang com a molt ℓ. Definim l'epimorfisme de grups abelians projecció $proj : n_1x_1 + \ldots + n_rx_r \mapsto n_r$ de $proj : M \to \mathbb{Z}$, (comproveu com exercici que $proj$ és efectivament un epimorfisme de grups abelians) on el nucli de $proj$ és justament un grup lliure de rang $\ell - 1$ generat per $x_1, \ldots, x_{\ell-1}$, i considerem la restricció del morfisme projecció al subgrup N, $proj|_N : N \to \mathbb{Z}$ que és morfisme de grups (exercici), on $ker(proj|_N)$ és un subgrup de $ker(proj)$ i per tant $ker(proj|_N)$ és un grup abelià lliure de rang com a molt $\ell - 1$ amb base $v_1, \ldots, v_s$ per hipòtesi d'inducció. Observem $im(proj|_N) = (t)$ (recordem im denota la imatge) per a cert t natural. Si $t = 0$ obtenim $ker(proj_{|N}) = N$ i per tant lliure. Si $t \neq 0$ triem $m_N \in N$ on $proj|_N(m_N) = t$, i deixem al lector demostrar que $N = v_1\mathbb{Z} + \ldots + v_s\mathbb{Z} + m_N\mathbb{Z}$ i $v_1, \ldots, v_s, m_N$ és una base per a N i per tant N és lliure de rang $s + 1 \leq \ell$. □

Teorema 1.56. *Sigui M un grup abelià lliure de rang N i sigui N un subgrup abelià de M. Llavors existeix una base $(y_1, \ldots, y_N)$ de M on $(d_1y_1, \ldots, d_my_m)$ és una base per a N on $m \leq M$ i $d_i \geq 1$ son naturals complint $d_1|d_2|\ldots|d_m$.*

Demostració. Considerem $\phi : M \to \mathbb{Z}^\ell$, via $\phi(\sum n_iy_i) = (n_1, \ldots, n_M)$, i deixem com exercici al lector que ϕ és un isomorfisme de grups abelians. És fàcil obtenir que $\phi(N)$ és una subxarxa de $\mathbb{Z}^\ell$ generat per certa base de N (ja que és un grup abelià lliure de rang $s \leq \ell$). Sigui B' una base de la subxarxa $\phi(N)$ respecte una base fixa B de $\mathbb{Z}^N$ que podem considerar la base "canònica", on escrivim $B = I_N$, $B' \in M_{N\times s}(\mathbb{Z})$ on les matrius columna de B' és una base de $\phi(N)$ a coordenades en la base canònica (és a dir $\phi(N) = \phi(\mathbb{Z}t_1 + \ldots + \mathbb{Z}t_s) = \mathbb{Z}\phi(t_1) + \ldots + \mathbb{Z}\phi(t_s)$ és una subxarxa de $\mathbb{Z}^\ell$ on $\phi(t_1), \ldots, \phi(t_s)$ és una base d'aquesta subxarxa on descrivim $\phi(t_j)$ descrivim per un element de $\mathbb{Z}^\ell$ respecte base $e_1 := (1, 0, \ldots, 0), \ldots, e_\ell := (0, \ldots, 0, 1)$ de $\mathbb{Z}^\ell$). Tenim que multiplicant per una matriu V unipotent obtenim que $B'V$ és una nova base de $\phi(N)$ respecte la mateixa base triada que expresem coordenades dels elements de la subxarxa respecte la xarxa $\mathbb{Z}^\ell$, veieu Lemma 1.30(.2). Ara si canviem base $\{e_1, \ldots, e_\ell\}$ de $\mathbb{Z}^\ell$ per una altra base $(y'_1, \ldots, y'_\ell)$ de $\mathbb{Z}^\ell$ correspon a multiplicar per una matriu U unipotent (on en U^{-1} la i-èssima columna corresponen a la descripció de y'_i en coordenades en $e_1, \ldots, e_\ell$) i per tant $UB'V$ és la descripció d'una base de $\phi(N)$ respecte la base nova de $\mathbb{Z}^N$ $\{y'_1, \ldots, y'_\ell\}$. Per la factorització Smith, podem triar U, V on $UB'V = Sm(B') = diag(d_1, \ldots, d_s, 0, ...)$ obtenim doncs el resultat entre $\phi(N)$ i $\mathbb{Z}^\ell$. Usant finalment l'isomorfisme ϕ s'obté el resultat sobre M i N com en l'enunciat del teorema. □

Definició 1.57. *Un grup abelià M s'anomena finit generat (i escriurem f.g.) si existeixen $m_1, \ldots, m_{\tilde{\ell}} \in M$ amb $\tilde{\ell} \in \mathbb{N}_{\geq 1}$ on $M = m_1\mathbb{Z} + \ldots + m_{\tilde{\ell}}\mathbb{Z}$, és a dir tot element de $m \in M$ es pot escriure com $m = \sum_{i=1}^{\tilde{\ell}} n_{i,m}m_i$ per a cents enters $n_{i,m}$.* [3]

Teorema 1.58. *Sigui M un grup abelià finit generat, llavors tenim un isomorfisme de grups β on*

$$M \cong^{\beta} \mathbb{Z}^t \bigoplus (\oplus_{i=1}^{s} \mathbb{Z}/(d_i))$$

on $d_1|d_2|\ldots|d_s$ naturals positius.

Demostració. Escrivim $M = m_1\mathbb{Z} + \ldots + m_{\tilde{\ell}}\mathbb{Z}$, i definim $\beta' : \mathbb{Z}^{\tilde{\ell}} \to M$ via $(m_1t_1+\ldots+m_{\tilde{\ell}}t_{\tilde{\ell}}) = \beta'(t_1, \ldots, t_{\tilde{\ell}})$ amb t_i enters. Deixem al lector demostrar que β' és un epimorfisme de grups abelians. Tenim llavors que $ker(\beta')$ és un subgrup abelià del grup abelià lliure $\mathbb{Z}^{\tilde{\ell}}$ i per tant és lliure, pel teorema anterior tenim una base de $\mathbb{Z}^{\tilde{\ell}}$: $y_1, \ldots, y_N$ on una base de $ker(\beta')$ s'escriu per: $d_1y_1, \ldots, d_sy_s$, per tant pel teorema d'isomorfia obtenim

$$\beta : \mathbb{Z}^{\ell}/ker(\beta') \to^{\cong} M$$

i $\mathbb{Z}^{\ell}/ker(\beta') \cong \mathbb{Z}/d_1 \oplus \ldots \oplus \mathbb{Z}/d_s \oplus \mathbb{Z}^{\tilde{\ell}-s}$ d'on el resultat amb $t = \tilde{\ell} - s$. □

Observació 1.59. Es pot demostrar que el t i $(d_1, \ldots, d_s)$ associats al grup abelià finit generat M del Teorema 1.58 són únics, i per tant s'obté una classificació de grups abelians finit generats. Al valor t s'anomena el rang del grup abelià finit generat M, on el sumatori $\bigoplus(\oplus_{i=1}^{s}\mathbb{Z}/(d_i))$ és un subgrup abelià finit i amb torsió i $\mathbb{Z}^t$ és un grup abelià lliure (i sense torsió).

[3] No confoneu finit generat amb la noció de lliure, fixem-nos que els $n_{i,m}$ aquí no són necessàriament únics.

Capítol 2

Enumeració.

2.1 Comptar en conjunts finits, consideracions inicials

Donat A un conjunt denotem per $|A|$ el cardinal del conjunt A, en particular si A és un conjunt finit, denota el nombre d'elements del conjunt A.

Principi 2.1 (d'adició)**.** *Siguin $A_1, \ldots, A_k$ conjunts finits disjunts dos a dos (és a dir $A_i \cap A_j = \emptyset$ per $i \neq j$) llavors*

$$|A_1 \cup \ldots \cup A_k| = \sum_{i=1}^{k} |A_i|.$$

Lema 2.2. *Sigui A un subconjunt d'un conjunt finit Ω, llavors*

$$|\Omega \setminus A| = |\Omega| - |A|,$$

on recordem que per dos conjunts C, D es defineix $C \setminus D := \{c \in C | c \notin D\}$.

Proof. Escrivim $\Omega = A \subset (\Omega \setminus A)$ com unió disjunta de dos conjunt, pel principi adició finalitzem. □

Lema 2.3 (propietat multiplicativa)**.** *Donats A, B conjunts finits llavors*

$$|A \times B| = |A| \cdot |B|.$$

Demostració. Escrivim com subconjunts disjunts $A \times B = \bigcup_{a \in A} \{a\} \times B$, pels principi d'adició i que $|\{a\} \times B| = |B|$. □

Principi 2.4 (regla del producte de compteig)**.** *Si tenim un procès en t etapes amb ordre: on en la primera etapa hi ha n_1-possibilitats, en la segona etapa hi ha n_2-possibilitats independentment de la tria en la 1a etapa, i successivament, on finalment en l'etapa t hi ha n_t-possibilitats independentment de les tries anteriors, llavors en aquest procediment hi ha exactament $n_1 \cdot n_2 \cdot \ldots \cdot n_t$ maneres diferents en aquest procés.*

Seleccions en elements d'un conjunt X de N-elements:

Permutacions: és una selecció d'elements d'un conjunt X on ordre de tria importa.
Combinacions: és una selecció d'elements d'un conjunt X on no importa ordre de tria (per tant correspon a l'elecció d'un subconjunt de X).

Distinguim les següents situacions de compteig:

- **Permutacions amb repetició.** El nombre de seleccions de k elements d'un conjunt X de N elements on podem repetir els elements del conjunt X ho denotem per PR_N^k. Fixem-nos que per la regla multiplicativa tenim k etapes, la primera etapa es triar un element del conjunt X i per tant tenim N possibilitats, en la segona etapa és igual ja que permetem repetició, iterant el procediment obtenim que

$$PR_N^k = N^k.$$

- **Permutacions sense repetició.** El nombre de seleccions de k elements d'un conjunt X de N elements on NO podem repetir els elements del conjunt X ho denotem per P_N^k. Pensem $k \leq N$ altrament no és possible cap selecció i per tant $P_N^k = 0$ si $k > N$. Altra vegada usant la regla multiplicativa el primer cas hi ha N possibilitats, i queda fer ara una selecció de $k-1$ elements en un conjunt de $N-1$ elements $P_N^k = N \cdot P_{N-1}^{k-1}$ iterant el procediment obtenim llavors

$$P_N^k = N \cdot (N-1) \ldots \cdot P_{N-(k-1)}^1 = N \cdot \ldots \cdot (N-k+1) = \frac{N!}{(N-k)!}.$$

- **Permutacions amb certes restriccions en repetició:** El nombre de seleccions de k elements del conjunt $X = \{a_1, \ldots, a_N\}$ d'N-elements on l'element a_i apareix $k_i \geq 0$-vegades en aquesta selecció complint $k = k_1 + \ldots + k_N$. Anomenem el nombre de totes aquestes permutacions per $P_N^{k_1,\ldots,k_N}$. Anem a calcular aquest valor.

  Fixem una d'aquestes seleccions de k elements, considerem el conjunt

$$Y = \{1_1, \ldots, 1_{k_1}, 2_1, \ldots, 2_{k_2}, \ldots, N_1, \ldots, N_{k_N}\}$$

  pensant $k_i \geq 1$ altrament no apareix. Observem que Y té exactament k elements on una selecció ordenada sense repetició del conjunt Y correspon a $k!$ possibilitats, ara si no distinguim els k_1 $1's$, ni els k_N $N's$ tenim que d'aquests $k!$ possibilitats s'ajunten en $k_1! \cdot \ldots \cdot k_N!$ i per tant

$$P_N^{k_1,\ldots,k_N} = \frac{k!}{k_1! \cdot \ldots \cdot k_N!}.$$

- **Combinacions sense repetició:** consisteix en l'elecció en el conjunt X d'agafar k elements sense importar l'ordre de tria, en particular correspon als diferents subconjunts de k elements que es poden triar en el conjunt X. La quantitat d'aquestes seleccions, o d'aquests subconjunts s'anota per $C_N^k = \begin{pmatrix} N \\ k \end{pmatrix}$.

D'eleccions possibles comptant l'ordre de tria n'hi ha P_N^k però n'hi ha exactament $k!$ iguals si no volem comptar l'ordre, d'on

$$C_N^k = \frac{P_N^k}{k!} = \frac{N!}{k!(N-k)!}.$$

- **Combinacions amb repetició:** consisteix amb les eleccions de k elements d'un conjunt de N elements podent fer repetició i sense importar ordre elecció. Mirem quantes possibles eleccion, hi ha, denotem aquests nombre per CR_N^k. Podem traslladar aquest problema de compteig via a posar k boles i cal col.locar $N-1$ pals separant entre elles, de manera que el nombre de boles entre pal i al $i+1$ correspon a l'element a_{i+1} repetit tantes vegades com les boles entre aquests dos pals, per tant correspon a triar entre número de boles i número de pals el lloc on posem els $N-1$ pals, és dir d'un conjunt d'elements $k+(N-1)$ triar-ne $N-1$ que corresponen a les posicions a posar els pals, per tant

$$CR_N^k = C_{k+(N-1)}^{N-1}.$$

Exemple 2.5. *Considera el conjunt* $\Lambda_{k,N} := \{(x_1, \ldots, x_N) \in \mathbb{N}^N | k = x_1 + \ldots + x_N\}$*, quin valor té* $|\Lambda_{k,N}|$*?*

Fixem-nos per $k = 4$ *i* $N = 3$ *podem pensar que correspon a posar 4 1's i cal posar dos pals per a separar per exemple* $1 + 1 + 2$ *correspondria a* $1|1|11$*, per tant aquest nombre correspon a un conjunt de* $k+(N-1)$ *elements on cal triar subconjunts de* $N-1$*-posicions on posar els pals, i per tant*

$$|\Lambda_{k,N}| = \left(\begin{array}{c} k+(N-1) \\ N-1 \end{array} \right).$$

2.1.1 Binomi Newton i primeres propietats nombre combinatori

Escrivim $(A+B)^N = (A+B) \cdot \ldots \cdot (A+B) = \sum_{j=0}^N n_j A^j B^{N-j}$, amb $N \geq 1$ natural, i calculem el valor n_j. Fixem-nos que per a obtenir $A^j B^{N-j}$ cal triar i parèntesis amb la A i $N-i$ parèntesis amb la B, per tant d'un conjunt N corresponent als N intervals $(A+B)$ cal triar-ne i sense importar ordre per tant obtenim

$$n_i = C_N^i.$$

Més en general si considerem $(A_1 + \ldots + A_N)^k$ el coeficient corresponents a grau k: $A_1^{k_1} \cdot \ldots \cdot A_N^{k_N}$ on $k = k_1 + \ldots + k_N$ correspon dels k intervals $(A_1 + \ldots + A_N)$ triar-ne k_1 amb A_1's, ..., k_N amb A_N's, per tant el nombre d'aquestes seleccions correspon a:

$$\frac{k!}{k_1! \ldots k_N!} = \left(\begin{array}{c} k \\ k_1, \ldots, k_N \end{array} \right).$$

Lema 2.6. *Tenim les següents propietats dels nombres combinatoris:*

1. $\left(\begin{array}{c} N \\ k \end{array} \right) = \left(\begin{array}{c} N \\ N-k \end{array} \right)$,

2. $\left(\begin{array}{c} N \\ k \end{array} \right) = \left(\begin{array}{c} N-1 \\ k \end{array} \right) + \left(\begin{array}{c} N-1 \\ k-1 \end{array} \right)$ *amb* $0 < k < N$.

3. *(adició paral.lela)* $\sum_{i=0}^{k} \left(\begin{array}{c} N+i \\ i \end{array} \right) = \left(\begin{array}{c} N+k+1 \\ k \end{array} \right)$

4. *Convolució de Vandermonde:* $\sum_{i=0}^{k} \left(\begin{array}{c} N \\ i \end{array} \right) \left(\begin{array}{c} M \\ k-i \end{array} \right) = \left(\begin{array}{c} N+M \\ k \end{array} \right)$.

Demostració. La primera propietats és clara, si volem argumentar-ho comptant-ho, serien paraules de longitud N on serien k zeros i $N-k$ 1's i podem permutar els 0's i 1's. Referent a la segona propietat, observem que els subconjunts de mida k d'un conjunt X de mida N es pot dividir amb els que NO contenen cert element A del conjunt X i per tant n'hi ha C_{N-1}^{k} i els que contenen A i per tant cal elegir $k-1$ elements en un conjunt de $N-1$ elements i per tant n'hi ha C_{N-1}^{k-1} obtenim la segona propietat.

Per la tercera propietat, es pot obtenir per iteració de la segona via:

$$C_N^k = C_{N-1}^k + C_{N-1}^{k-1} = C_{N-1}^k + C_{N-2}^{k-1} + C_{N-2}^{k-2} = \ldots = \sum_{j=1}^{k+1} C_{N-j}^{k-j+1}.$$

Per a demostrar la convolució de Vandermonde, sol observem que si tenim N boles blanques i M boles negres, i ajuntem-les amb un conjunt de $N+M$ boles (pensem que podem distingir totes les boles) volem triar exactament i boles blanques i $k-i$ boles negres que correspon a $\left(\begin{array}{c} N \\ i \end{array} \right) \left(\begin{array}{c} M \\ k-i \end{array} \right)$ seleccions, recorrent totes les possibles subconjunts de k elements en les $N+M$ boles totals i com una tria, triarem i boles blanques i $k-i$ boles negres obtenim el resultat. □

2.1.2 Principi inclusió-exclusió

Principi 2.7. *Donats dos conjunts finits A, B, llavors*

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

Demostració. Escrivim $A \cup B$ com unió disjunta de $(A \setminus B) \cup (B \setminus A) \cup (A \cap B)$ i observem que $(A \setminus B) = A \setminus (A \cap B)$ i $(B \setminus A) = B \setminus (A \cap B)$, pel lema 2.2 tenim $|A \setminus (A \cap B)| = |A| - |A \cap B|$, d'on obtenim el resultat. □

Principi 2.8 (d'inclusió-exclusió)**.** *Siguin $A_1, \ldots, A_N$ N conjunts finits. Llavors*

$$|A_1 \cup \ldots \cup A_N| =$$

$$\sum_{i=1}^{N} |A_i| - \sum_{i<j} |A_i \cap A_j| + \ldots + (-1)^{r-1} \sum_{i_1<\ldots<i_r} |A_{i_1} \cap \ldots \cap A_{i_r}| + \ldots + (-1)^{N-1} |A_1 \cap \ldots \cap A_N|. \tag{2.1}$$

Demostració. Triem $x \in A_1 \cup \ldots A_N$ arbitrari que es troba en exactament $t \leq N$ dels N conjunts $A_1, \ldots, A_N$. Provarem que x està comptat exactament un cop en l'expressió (2.1).

Efectivament, en el terme $\sum_{i=1}^{N} |A_i|$ l'element x està comptat exactament t vegades.

En el segon terme $\sum_{i<j} |A_i \cap A_j|$ com l'element x que es troba en t conjunts es trobarà exactament en $\left(\begin{array}{c} t \\ 2 \end{array} \right)$ factors i per tant comptat aquest nombre combinatori.

En general en el terme r (amb $r \leq t \leq N$) l'element x apareix comptat exactament $\left(\begin{array}{c} t \\ r \end{array} \right)$.

Per tant en l'expressió (2.1) l'element x surt comptat exactament

$$\left(\begin{array}{c} t \\ 1 \end{array} \right) - \left(\begin{array}{c} t \\ 2 \end{array} \right) + \ldots + (-1)^{r-1} \left(\begin{array}{c} t \\ r \end{array} \right) + \ldots + (-1)^{t-1} \left(\begin{array}{c} t \\ t \end{array} \right)$$

i observem que $0 = (1 + (-1))^t = \sum_{j=0}^{t} (-1)^j \left(\begin{array}{c} t \\ j \end{array} \right)$, per a concloure que està comptat exactament un cop en (2.1). □

Exemple 2.9 (Desarreglaments)**.** *Considerem un conjunt finit $X = \{a_1, \ldots, a_N\}$ d'N-elements. Considerem una permutació del conjunt X:* **per** $= a_{i_1} a_{i_2} \ldots a_{i_N}$. *Un desarreglament per a* **per** *és una permutació del conjunt X on cap element es troba al seu lloc, és a dir $b = a_{b_1} \ldots a_{b_N}$, diem b és un desarreglament per a* **per** *si $a_{b_j} \neq a_{i_j}$ per a tot $j = 1, \ldots, N$.*

Per exemple, si $X = \{1, 2, 3, 4\}$ i **per** $= 1234$*, tenim que* 4123 *és un desarreglament, en canvi* 1423 *no ho és.*

Qüestió 2.10. *Quants desarreglaments hi ha per a la permutació fixada* **per** *del conjunt X on X és el conjunt $\{a_1, \ldots, a_N\}$ amb N elements?*

Escrivim per A_s al conjunt de permutacions de X que deixen fix l'element a_{i_s} en el lloc s. Si denotem per D_{per} els desarreglaments de **per** *del conjunt X obtenim que*

$$D_{per} = S_N \setminus (\bigcup_{s=1}^{N} A_i)$$

on S_N denoten totes les permutacions del conjunt X (que n'hi ha $N!$). Fixem-nos que $|A_s| = (N-1)!$ on tenim lloc s fixat per l'element a_{i_s} però les altres possicions tenim llibertat per a distribuir $N-1$ elements amb ordre. Similarment obtenim que $|A_{i_1} \cap \ldots A_{i_r}| = (N-r)!$. Per tant pel principi d'inclusió-exclusió obtenim

$$|D_{per}| = N! - \left(\begin{array}{c} N \\ 1 \end{array} \right) (N-1)! + \ldots + (-1)^r \left(\begin{array}{c} N \\ r \end{array} \right) (N-r)! + \ldots + (-1)^N \left(\begin{array}{c} N \\ N \end{array} \right) =$$

$$N! \left(1 - \frac{1}{1!} + \frac{1}{2!} + \ldots + (-1)^r \frac{1}{r!} + \ldots + (-1)^N \frac{1}{N!} \right)$$

i per tant obtenim el nombre de desarreglaments. [1]

[1] Recordeu que $e^{-1} = (1 - \frac{1}{1!} + \frac{1}{2!} + \ldots + (-1)^r \frac{1}{r!} + \ldots) = \sum_{i \geq 0} \frac{1}{i!}$.

2.1.3 Principi de Dirichlet (o del colomar)

Principi 2.11 (de Dirichlet)**.** *En una selecció de $k+1$ elements o més, d'un conjunt que té k elements, almenys algun element apareix dos cops o més.*

Anem a donar un exemple d'aquest principi.

Lema 2.12. *Donada una successió creixent: $\{a_j\}_{j=1}^{2n}$ de $2n$ nombres naturals diferents on $1 \leq a_j \leq 3n$, és a dir $1 \leq a_1 < \ldots < a_{2n} \leq 3n$. Llavors existeix $i, j \leq 2n$ amb $a_i < a_j$ complint que $a_i - a_j = n - 1$.*

Demostració. Observa que $a_1, \ldots, a_{2n}, a_1 + (n-1), \ldots, a_{2n} + (n-1)$ són $4n$ números entre 1 i $4n-1$ per tant hi ha dos números iguals per tant existeix i, j on $a_j = a_i + (n-1)$. □

Principi 2.13 (de Dirichlet, II)**.** *En una selecció de k elements en un conjunt que té N elements (amb $N \leq k$), llavors hi ha algún element que apareix almenys $[\frac{k}{N}]$ vegades (on $[t]$ denota aquí la part entera del nombre real t).*

Anem a fer-ne una aplicació

Proposició 2.14 (Erdös-Szekeres, 1935)**.** *En una successió qualsevol de N^2+1 enters diferents o bé hi ha una subsuccessió estrictament creixent de $N+1$ elements o bé hi ha una subsuccessió estrictament decreixent de $N+1$ elements.*

Demostració. Sigui $a_1, \ldots, a_{N^2+1}$ successió original. Per a cada i, denotem per c_i la longitdu de la subsuccessió creixent que comença per a_i. Si algun c_i és més gran que $N+1$ ja finalitzem. En cas contrari, obtenim N^2+1 enters: $c_1, \ldots, c_{N^2}, c_{N^2+1}$ entre 1 i N, per tant pel principi de Dirichlet, hi ha $[\frac{N^2+1}{N}] = N+1$ enters iguals, suposem doncs que

$$c_{i_1} = \ldots = c_{i_{N+1}} \text{ amb } i_1 < \ldots < i_{N+1}$$

Afirmem que $a_{i_1}, \ldots, a_{i_{N+1}}$ és una subsuccessió decreixent. Efectivament, si no ho fos existiria k on $a_{i_k} < a_{i_{k+1}}$ ara usant que la subsuccessió creixent més llarga que s'inicia per $a_{i_{k+1}}$ té longitud $c_{i_{k+1}}$ obtenim una subsuccessió creixent a partir de a_{i_k} de longitud $c_{i_{k+1}} + 1$, per tant $c_{i_k} \geq c_{i_{k+1}} + 1$ en contradicció que aquests valors eren iguals. □

2.2 Grups actuant sobre un conjunt X definint un conjunt quocient

Definició 2.15. *Sigui X un conjunt i G un grup, diem que G actúa en X (per l'esquerra) si tenim una aplicació*

$$h : G \times X \to X$$

$$(g, x) \mapsto g * x := h(g, x)$$

que compleix les propietats següents:

1. $h(g_1 \cdot g_2, x) = (g_1 \cdot g_2) * x = g_1 * (g_2 * x) = h(g_1, h(g_2, x))$,
2. $h(1, x) = 1 * x = x$.

En aquesta situació definim $G_x := \{g \in G | h(g,x) = x\}$ *i* $X_g := \{x \in X | h(g,x) = x\}$.

Observació 2.16. *De manera similar diem que un grup* G *actúa en* X *per la dreta si demanem que* h *compleixi* $h(g_1 \cdot g_2, x) = h(g_2, h(g_1, x))$ *(i* $h(1,x) = x$*). Enlloc d'escriure la relació donada per* h *amb la notació de la definició anterior que seria:* $(g_1 \cdot g_2) * x = g_2 * (g_1 * x)$*, ho escriurem* h *per accions per la dreta mitjançant* $h(g,x) =: x * g$ *on llavors és més natural la propietat requerida per l'apliació* h *escrivint-se en accions per la dreta mitjançant* $x * (g_1 \cdot g_2) = (x * g_1) * g_2$.

Lema 2.17. *El subconjunt* G_x *de* G *és un subgrup de* G.

Demostració. Recordem que donat un grup G amb l'operació $\cdot$ [2], un subconjunt $H \subset G$ és un subgrup de G si H amb l'operació $\cdot$ és un grup, i és equivalent a demostrar que $\forall h_1, h_2 \in H$ llavors $h_1 \cdot h_2^{-1} \in H$ i $1_G \in H$.

Per tant per a demostrar que el subconjunt de G donat per G_x és un subgrup, hem de veure que donats $g_1, g_2 \in G_x$ llavors $g_1 \cdot g_2^{-1} \in G_x$ i $1_G \in G_x$ (on aquest últim és clar). Ho demostrem aquí quan G actúa en X per l'esquerra (si ho fa per la dreta exercici al lector).

Observem primer si pensem $g *_G x = h(g,x)$, fixem-nos que la propietat $g_1 *_G (g_2 * x) = (g_1 \cdot g_2) *_G x$ s'escriu com $h(g_1, h(g_2, x)) = h(g_1 g_2, x)$.

D'aquí si $g \in G_x$ tenim $h(g,x) = x$, i observem llavors $g^{-1} *_G x = h(g^{-1}, x) = h(g^{-1}, h(g,x)) = h(g^{-1}g, x) = h(1,x) = x$, per tant $g^{-1} \in G_x$.

Agafem ara $g_1, g_2 \in G_x$ i estudiem $(g_1 g_2^{-1}) *_G x = h(g_1 g_2^{-1}, x) = h(g_1, h(g_2^{-1}, x))$ com $h(g_2^{-1}, x) = x$ per ser $g_2^{-1} \in G_x$ tenim $(g_1 g_2^{-1}) *_G = h(g_1, x) = x$ on l'última igualtat prové que $g_1 \in G_x$, per tant el resultat. □

Definició 2.18. *Sigui* G *un grup on actúa en* X *(per l'esquerra). Donat* $x_1, x_2 \in G$ *diem que* $x_1 \sim_G x_2$ *si i només si existeix* $g \in G$ *on* $g * x_1 = x_2$.
[3]

Lema 2.19. *El conjunt* X *amb una acció pel grup* G*, llavors* $\sim_G$ *dóna una relació d'equivalència en el conjunt* X.

Demostració. Fem la demostració quan l'acció és per l'esquerra (exercici al lector quan l'acció és per la dreta).

Transitiva: si $x_1 \sim x_2$ i $x_2 \sim x_3$ tenim $x_2 = g_1 * x_1$ i $x_3 = g_2 * x_2$ per certs $g_2, g_1 \in G$, d'on $(g_2 \cdot g_1) * x_1 = g_2 * (g_1 * x_1) = g_2 * x_2 = x_3$ i per tant $x_1 \sim x_3$.
Simètrica: si $x_1 \sim x_2$ tenim $x_2 = g_1 * x_1$, per tant $g_1^{-1} * x_2 = g_1^{-1} * (g_1 * x) = (g_1^{-1} \cdot g_1) * x_1 = 1 * x_1 = x_1$ i per tant $x_2 \sim x_1$.
Reflexiva: clarament $x \sim x$ de la propietat que $1 * x = x$. □

Observació 2.20. *Donat un grup* X *amb operació* $\bullet$*, i* M *un subgrup de* X *podem considerar* $\ell_l : M \times X \to X$ *donat per* $\ell_l(m,x) := m \bullet x$*. Fixem-nos que això dóna l'acció de* M *en* X *i podem formar conjunt quocient de classes laterals del grup* X *pel subgrup* M *per l'esquerra. Similarment podem considerar l'acció per la dreta* $\ell_r(m,x) := x \bullet m$*, i fer el conjunt quocient del grup* X *pel*

[2] Un conjunt G amb una operació $\cdot$ és diu que és un grup si $(G, \cdot)$ satisfà la propietat associativa, element neutre, i tot element té invers. En cas que l'operació sigui commutativa diem que $(G, \cdot)$ és un grup abelià.

[3] En cas que l'acció de G sobre X sigui per la dreta, definim $x_1 \sim_G x_2$ si i només si $h(g, x_1) = x_2$ (és a dir $h(g, x_1) = x_1 * g = x_2$).

subgrup M per la dreta, correspon al que s'anomena classes lateral per la dreta del subgrup M de X. Problema: quina relació hi ha entre les classes laterals del grup X pel subgrup M per l'esquerra i per la dreta, en particular entre aquests dos conjunts quocients?

Donat X amb una acció per un grup G podem considerar el conjunt quocient $\mathcal{M} = X/\sim_G$.

Qüestió 2.21. *Com calcular $|\mathcal{M}|$?*

Lema 2.22 (Burnside)**.** *Sigui X un conjunt finit i G un grup finit que actúa en X. Llavors*

$$|\mathcal{M}| = \frac{1}{|G|}\sum_{g\in G}|X_g| = \frac{1}{|G|}\sum_{x\in X}|G_x|.$$

Demostració. Fem la demostració per accions per l'esquerra (per la dreta exercici al lector).

Fixem-nos que

$$\sum_{x\in X}|G_x| = |\{(x,g) : g*x = x\}| = \sum_{g\in G}|X_g|$$

per tant obtenim $\sum_{g\in G}|X_g| = \sum_{x\in X}|G_x|$.

Considerem la classe de x, via $[x] = \{g*x | g\in G\} \subset X$ i observem que $|[x]| = \frac{|G|}{|G_x|}$ [4] i obtenim

$$|G| = |[x]||G_x| = \sum_{y\in[x]}|G_y|$$

ja que si $y\in[x]$ tenim $|G_x| = |G_y|$[5]. Per tant:

$$|\mathcal{M}|\cdot|G| = \sum_{[x]\in\mathcal{M}}\sum_{y\in[x]}|G_y| = \sum_{x\in X}|G_x|.$$

□

Qüestió 2.23. *Fem collarets amb N boles i cada bola podem usar c colors. Quants collarets són possibles amb els valors N i c fix?*

[4] Fixem-nos que $[x] = \{x = g_0*x, g_1*x, \ldots, g_s*x\}$ per a certs $g_i\in G$, amb $g_i*x \neq g_j*x$. Considerem ara $\cup_{i=1}^{s} g_iG_x \subset G$, fixem-nos que $g_iG_x \cap g_jG_x = \emptyset$ si $i\neq j$ ja que sino, obtenim que $g_ih = g_jh'$ amb $h,h'\in G_x$ i per tant $g_j^{-1}g_i = h'h^{-1}\in G_x$, per tant $g_j*x = g_j*((g_j^{-1}g_i)*x) = (g_jg_j^{-1})*(g_i*x) = g_i*x$. D'aquí obtenim que $\cup_{i=0}^{s} g_iG_x$ és una unió disjunta d'elements del grup G. Afirmem que aquesta unió disjunta és exactament el grup G i que $|g_iG_x| = |G_x|$, i un cop demostrat aquesta afirmació obtenim que $|G| = |G_x||[x]|$ com volem detallar en aquest peu de pàgina. Fixem-nos $t : G_x \to g_iG_x$ amb $t(g) = g_ig$ és una bijecció amb l'aplicació inversa $u(g) = g_i^{-1}g$ i per tant $|G_x| = |g_iG_x|$. Sigui ara $g\in G$ tenim que $g*x = g_i*x$ per a cert g_i i per tant $g_i^{-1}g\in G_x$ d'on obtenim que $g\in g_iG_x$ i per tant $G = \cup_{i=0}^{s} g_iG_x$.

[5] Recordem $y\in[x]$ és de la forma $y = g_i*x$ per cert $g_i\in G$ fixem-nos que $g_i^{-1}G_yg_i \subseteq G_x$ ja que $(g_i^{-1}h_yg_i)*x = (g_i^{-1}h_y)*y = g_i^{-1}*y = g_i^{-1}*(g_i*x) = (g_i^{-1}g_i)*x = x$ per a tot $h_y\in G_y$, d'on $|g_i^{-1}G_yg_i| \leq |G_x|$. Ara, veiem que $(g_iG_xg_i^{-1})*y = y$: efectivament $(g_ih_xg_i^{-1})*y = (g_ih_xg_i^{-1})*(g_i*x) = (g_ih_xg_i^{-1}g_i)*x = g_i(h_x*x) = g_i*x = y$ per a tot $h_x\in G_x$ per tant $|g_iG_xg_i^{-1}| \leq |G_y|$, deixo com exercici al lector demostrar que $|g_iG_xg_i^{-1}| = |G_x|$ i $|g_i^{-1}G_yg_i| = |G_y|$.

Per exemple per $N = 4$ i $c = 2$ tenim 6 possibilitats de colors. [Hem fet el dibuix a classe]

Formalitzem aquest exemple en un context matemàtic. Considerem una aplicació $f : X \to C$ on $X = \{a_1, \ldots, a_N\}$ correspon a les N boles, i C el conjunt de colors a usar, d'una aplicació f concreta obtenim un collaret (hem estirat el collaret i diem possició 1 fins possició N). No obstant si fem una rotació en un collaret, obtenim el mateix collaret però pensant com aplicació a la possició $i + j$ li assignem el color que tenia anteriorment la possició i (on j es fix de la rotació produïda), per tant tenim una l'aplicació del conjunt X al conjunt C diferent de la f inicial, fixem-nos que obtenim el mateix collaret no obstant l'aplicació que associariem és diferent, volem doncs identificar aquestes diferents aplicacions que donen el mateix collaret. Fixem-nos que una rotació de i posicions correspon a $g_i : X \to X$ via $g_i(x_j) = x_{j+i \ mod \ N}$ obtenint que el collar donat per f i $f \circ g_i$ coincideixen (on pensem possició N enlloc de possició 0 en fer mòdul N). Anem a relacionar aquest problema de compteig a l'acció d'un grup en el conjunt de les aplicacions entre el conjunt X al conjunt C.

Considerem $X = \{a_1, \ldots, a_N\}$ i sigui G un grup que el pensem com un subgrup de S_X, on S_X denota totes les aplicacions bijectives del conjunt X e identificarem S_X amb S_N el grup de permutacions del conjunt $\{1, \ldots, N\}$ amb l'assignació natural. Donat un conjunt C, escrivim per X^C al conjunt de totes les aplicacions del conjunt X al conjunt C, definim:

$$comp : G \times X^C \to X^C$$

$$(g, f) \mapsto comp(g, f) := f \circ g$$

on $\circ$ denota la composició d'aplicacions.

Lema 2.24. *X^C amb l'aplicació comp defineix una acció (per la dreta) del grup G en X^C, i per tant podem formar el conjunt quocient $X^C/\sim_G$ (on $f_1 \sim_G f_2$ amb $f_1, f_2 \in X^C$ sii existeix $g \in G$ on $comp(g, f_1) = f_1 \circ g = f_2$).*

Demostració. Escrivim $comp(g, f) = f *_1 g (= f \circ g)$, cal justificar $(f *_1 g_1) *_1 g_2 = f *_1 (g_1 \cdot g_2)$ per a tot $f \in X^C$ i $\forall g_1, g_2 \in G$, i també la igualtat $f *_1 1 = f$.

Clarament $f *_1 1 = f \circ id = f$, ja que $1 \in G$ com una aplicació bijectiva en el conjunt X que té N elements és l'aplicació identitat. Fixem-nos ara $g_1 \cdot g_2$

correspon a la composició de les aplicacions bijectives de X en X donades per g_1 i g_2, tenim llavors: $f *_1 (g_1 \cdot g_2) = f \circ (g_1 \circ g_2) = (f \circ g_1) \circ g_2 = (f *_1 g_1) \circ g_2 = (f *_1 g_1) *_1 g_2$ i per tant obtenim una acció de grup. □

Teorema 2.25 (d'enumeració de Pólya)**.** *En les condicions anteriors tenim*

$$|X^C/\sim_{*_1}| = \frac{1}{|G|}\sum_{g\in G}|C|^{c(g)}$$

on $c(g)$ és el nombre de cicles disjunts de l'element g pensant aquest $g \in G$ com un element del grup de permutacions amb N-elements $S_X \cong S_N$ (on $|X| = N$).

Demostració. Apliquem al lema de Burnside 2.22, i tenim

$$|X^C/\sim_{*_1}| = \frac{1}{|G|}\sum_{g\in G}|(X^C)_g|.$$

Anem a calcular $|(X^C)_g|$.

Considerem $g \in S_X \cong S_N$, podem escriure amb poductes de cicles disjunts:

$$(a, g(a), \ldots)(b, g(b), \ldots)...$$

on $a, b, g^j(a), g^j(b) \in X$, si $f \in (X^C)_g$ vol dir que $f \circ g = f$ per tant tenim que $f(a) = f(g(a)) = \ldots$, $f(b) = f(g(b)) = \ldots$, per tant f és constant en els diferents cicles disjunts de g, i qualsevol funció f que és constant en els cicles disjunts de g com element de S_N pertany a $(X^C)_g$, i les possibles eleccions d'aquestes funcions és justament $|C|^{c(g)}$ on $c(g)$ és el nombre de cicles disjunts de l'element $g \in S_X$ (on els cicles de longitud 1 també compten), ja que es assignar un mateix valor del conjunt C per tots els elements de X del cicle $(a, g(a), \ldots)$, igualment un mateix valor de C per tots els elements de X del cicle $(b, g(b), g^2(b), \ldots)$, d'on pel resultat de permutacions amb repetició obtenim que $|(X^C)_g| = |C|^{c(g)}$, i per tant el resultat. □

Exemple 2.26. *Resolem ara la pregunta dels collarets diferents que podem formar amb N boles i on cada bola la podem decorar amb c colors diferents (on podem repetit com volem els colors).*

Fem un cas concret $X = \{bola_1, bola_2, bola_3, bola_4\}$ que el designem per $X = \{1, 2, 3, 4\}$ i $C = \{color_1, color_2\}$ i per abús de notació podem pensar $C = \{1, 2\}$. Aquest cas G que actua correspon a $g_i(x) = x + i(mod\ 4)$ i està generat per g_1 el grup G que té el cicle $g_1 = (1, 2, 3, 4)$, fixem-nos que g_2 correspon al cicle $(1, 3)(2, 4)$, g_3 al cicle $(1, 3, 2, 4)$ i $g_4 = id$ i per tant al cicle $(1)(2)(3)(4)$, per tant el nombre de collarets és

$$\frac{1}{4}(2^1 + 2^2 + 2^1 + 2^4) = 6$$

6 collarets, com sabíem.

Exercici al lector per descriure la situació general.

2.3 Funcions generadores

Donat $\mathbb{K}$ un cos, denotem per $\mathbb{K}[[x]] := \{\sum_{i\in\mathbb{N}} k_i x^i | k_i \in \mathbb{K}\}$ on hi definim una suma i producte mitjançant:

$$(\sum_{i\geq 0} u_i x^i) + (\sum_{j\geq 0} v_j x^j) = U(x) + V(x) := \sum_{k\geq 0}(u_k + v_k)x^k$$

$$(\sum_{i\geq 0} u_i x^i) \cdot (\sum_{j\geq 0} v_j x^j) = U(x) \cdot V(x) := \sum_{k\geq 0} c_k x^k$$

on $a_i, b_i \in \mathbb{K}$ i $c_i := \sum_{t=0}^{i} u_t v_{i-t}$.

Lema 2.27. *$\mathbb{K}[[x]]$ amb la suma i producte anterior defineix un anell commutatiu amb unitat.*

Demostració. Exercici al lector. □

Anomenem per $\mathbb{K}[[x]]$ l'anell de les series formals en la variable x en el cos $\mathbb{K}$.

Observació 2.28. *L'anell $\mathbb{K}[[x]]$ és pot definir com la completació de l'anell $\mathbb{K}[x]$ respecte la topologia $||_x$ introduïda el primer dia de classe.*

Lema 2.29. *Donat $U(x) = \sum_{n\geq 0} u_n x^n \in \mathbb{K}[[x]]$ és invertible en $\mathbb{K}[[x]]$ si i només si $u_0 \neq 0$.*

Demostració. $\Rightarrow$ Si $U(x)$ invertible, existeix $V(x)$ complint que $\sum_{n\geq 0} c_n x^n = U(x) \cdot V(x) = 1$ on $1 = c_0 = u_0 v_0$ i $0 = c_n$ with $n > 0$, en particular $u_0 \neq 0$.

$\Leftarrow$ Volem construir $V(x)$ on $\sum_{n\geq 0} c_n x^n = U(x) \cdot V(x) = 1$, tenim $1 = u_0 v_0$ d'on $v_0 = u_0^{-1}$, sabent v_n per $n \leq K$, obtenim el valor per v_{K+1} ja que $0 = c_{K+1} = v_{K+1}u_0 + v_K u_1 + \ldots + u_{K+1}v_0$ i podem obtenir v_{K+1}, de forma recursiva i per tant obtenim $V(X)$. □

Exemple 2.30. *Fixem-nos la sèrie formal f escrita per $\sum_{n\geq 0} x^n$ és invertible en $\mathbb{K}[[x]]$ pel lema anterior. Anem a calcular $f^{-1} \in \mathbb{K}[[x]]$.*

Escrivim $f^{-1} := \sum_{n\geq 0} v_n x^n$ e imposem $1 = f \cdot f^{-1}$ on obtenim $v_1 = 1$, i seguint notaci'o demostració del lemma $v_{K+1} = -\sum_{k=0}^{K} v_k$, on clarament $v_1 = -1$ i $v_j = 0$ per $j \geq 2$ i per tant $f^{-1} = (1 - x)$ on escriurem

$$f = 1 + x + x^2 + x^3 + \ldots = \sum_{k\geq 0} x^k = (1-x)^{-1} = \frac{1}{1-x}.$$

Una altra manera d'argumentar seria considerar com $\mathbb{K}[[x]]$ és una completació respecte valor absolut no-arquimedià $||_x$ de $\mathbb{K}[x]$ tenim

$$(1 + \ldots + x^N)(1 - x) = 1 - x^{N+1}$$

i com successió $A_N := \sum_{i=0}^{N} x^i$ és convergent en $\mathbb{K}[[x]]$ amb el valor absolut anomenat i $B_N := 1 - x$ tenim $C_N = A_N \cdot B_N = 1 - x^{N+1}$ convergeix a 1, i per tant obtenim prenent limit que $(\sum_{k\geq 0} x^k)(1 - x) = 1$ en $\mathbb{K}[[x]]$. Per aquest curs usarem la manera formal per fer-ne operacions sense usar-ne la topologia via un valor absolut no arquimedià.

Definició 2.31. *Donada una successió $(a_n)_{n\in\mathbb{N}}$ o una aplicació $f : \mathbb{N} \to \mathbb{K}$ complint $f(n) = a_n$, denotem la funció generadora associada a la successió $(a_n)_n$ o a l'aplicació f a la sèrie formal següent*

$$u(x) := \sum_{n\in\mathbb{N}} a_n x^n \in \mathbb{K}[[x]]$$

Exemple 2.32. *Considerem el polinomi (en particular sèrie formal) $U_N(x) := (1+x)\cdot\ldots\cdot(1+x) = (1+x)^N = \sum_{k\geq 0}\left(\begin{array}{c} N \\ k \end{array}\right)x^k$ on definim $\left(\begin{array}{c} N \\ k \end{array}\right) = 0$ si $k > N$.*

Fixem-nos que $U_N(x)$ és la **funció generadora** *de la successió $a_t = \left(\begin{array}{c} N \\ t \end{array}\right)$ amb N fix.*

Això ens permet trobar igualtats no tant evidents. Per exemple de

$$U_{2N}(x) = (U_N(x))^2$$

- $\left(\begin{array}{c} 2N \\ N \end{array}\right)$, *coeficient de grau N en variable x, en l'expressió $U_{2N}(x)$.*
- *coeficient de grau N en variable x de $(U_N(x))^2$ correspon a la suma de totes les possibilitats de triar exactament k x's en el primer $U_N(x)$ entre els N-factors $(x+1)$ i de triar-ne exactament $N-k$ valors x's del segon $U_N(x)$ (que té N-factors $(x+1)$), i per tant correspon a*

$$\sum_{k=0}^{N}\left(\begin{array}{c} N \\ k \end{array}\right)\left(\begin{array}{c} N \\ N-k \end{array}\right) = \sum_{k=0}^{N}\left(\begin{array}{c} N \\ k \end{array}\right)^2$$

per tant obtenim la igualtat:

$$\left(\begin{array}{c} 2N \\ N \end{array}\right) = \sum_{k=0}^{N}\left(\begin{array}{c} N \\ k \end{array}\right)^2.$$

Definició 2.33. *Donada una sèrie formal $U(x) = \sum_{k\geq 0} u_k x^k \in \mathbb{K}[[x]]$, es defineix la sèrie formal derivada de $U(x)$ a la sèrie*

$$U'(x) := \sum_{k\geq 1} k u_k x^{k-1} \in \mathbb{K}[[x]].$$

Observació 2.34. *Es pot demostrar que si $U(x) \in \mathbb{R}[x]$ té radi de convergència r al voltant de $x = 0$ amb la noció anàlisi amb el valor absolut arquimedià $||_\infty$, llavors $U'(x)$ coincideix amb la funció derivada de la funció $U(x)$ en un entorn del zero (penseu per exemple el desenvolupament de Mac Lauren).*

Exemple 2.35. *$U_N(x)' = \sum_{k\geq 1} k\left(\begin{array}{c} N \\ k \end{array}\right)x^{k-1}$, que és la derivada usual de $(1+x)^N$ que és $NU_{N-1}(x)$ d'aquí:*

$$N2^{N-1} = N(1+1)^{N-1} = NU_{N-1}(1) = \sum_{k\geq 1} k\left(\begin{array}{c} N \\ k \end{array}\right)1^{k-1} = \sum_{k\geq 1} k\left(\begin{array}{c} N \\ k \end{array}\right).$$

Anem a veure més exemples d'aplicacions de funcions generadores diferents que l'obtinguda per a $U_N(x)$.

Exemple 2.36. *Estudiem a quina successió associada a la funció generadora donada per la sèrie (en aquest cas un polinomi)* $(1+x+x^2)^N$ *amb* N *un natural fixat. El coeficient* x^k *compte la manera d'escollir* 1,x *o* x^2 *en cadascú dels* N *parèntesis* $(1+x+x^2)$ *on la suma d'exponents sigui exactament* k*, és a dir el seu coeficient és:*

$$\Lambda_{k,N,(2,\ldots,2)} = \{(r_1,\ldots,r_N) \in \mathbb{N}^N | 0 \leq r_i \leq 2 \sum_{i=1}^{N} r_i = k\}.$$

Per exemple, calculem $|\Lambda_{11,20,(2,\ldots,2)}| = 18062160$*. Ens ajudem d'un manipulador algebraic com Magma online calculator* ***http://magma.maths.usyd.edu.au/calc/*** *i si escrivim per exemple com INPUT:*

```
k<x>:=PolynomialRing(Rationals());
p:=1+x+x^2;
(p)^(20);
```

obtenim com OUTPUT el resultat:

```
x^40 + 20*x^39 + 210*x^38 + 1520*x^37 + 8455*x^36 + 38304*x^35 + 146490*x^34 +
484500*x^33 + 1409895*x^32 + 3656360*x^31 + 8533660*x^30 + 18062160*x^29 +
34880770*x^28 + 61757600*x^27 + 100640340*x^26 + 151419816*x^25 +
210859245*x^24 + 272290140*x^23 + 326527350*x^22 + 363985680*x^21 +
377379369*x^20 + 363985680*x^19 + 326527350*x^18 + 272290140*x^17 +
210859245*x^16 + 151419816*x^15 + 100640340*x^14 + 61757600*x^13 +
34880770*x^12 + 18062160*x^11 + 8533660*x^10 + 3656360*x^9 + 1409895*x^8 +
484500*x^7 + 146490*x^6 + 38304*x^5 + 8455*x^4 + 1520*x^3 + 210*x^2 + 20*x +1
```

i d'aquí n'extreiem el resultat.

Exemple 2.37. *Anem a trobar una fórmula tancada per a la successió corresponent a la sèrie formal* $\frac{1}{(1-x)^N} = (1+x+\ldots)^N$ *amb* N *un natural* ≥ 1 *fixat.*

Fixem-nos que la successió corresponent a la funció generadora $(1+x+\ldots)^N$*, el coeficient* x^k *compte la manera d'escollir* 1,x,*... en cadascú dels* N *parèntesis* $(1+x+\ldots)$ *on la suma dels exponents sigui* k*, és a dir:*

$$\Lambda_{k,N} = \{(r_1,\ldots,r_N) \in \mathbb{N}^N | \sum_{i=1}^{N} r_i = k\},$$

i en la secció anterior hem demostrat que $|\Lambda_{k,N}| = \left(\begin{array}{c} k+(N-1) \\ k \end{array} \right)$ *i per tant*

$$\frac{1}{(1-x)^N} = (\sum_{k\geq 0} x^k)^N = \sum_{k\geq 0} \left(\begin{array}{c} k+(N-1) \\ k \end{array} \right) x^k.$$

Definició 2.38. *La funció generadora exponencial per una successió* $(c_n)_n$ *de números reals correspon a la sèrie formal:*

$$E(X) := \sum_{n\geq 0} \frac{c_n}{n!} x^n \in \mathbb{R}[[x]].$$

Lema 2.39. *Si $E(x)$ i $G(x)$ son funcions generadores exponencials per successions $(c_n)_n$ i $(g_n)_n$ respenctivament, llavors $E(x)G(x)$ és la funció generadora exponencial per a la successió $(prod_n)_n$ on*

$$prod_n = \sum_{k=0}^{n} \left(\begin{array}{c} n \\ k \end{array} \right) c_k g_{n-k}.$$

Demostració. Tenim la igualtat següent:

$$\left(\sum_{n\geq 0} \frac{c_n}{n!} x^n \right) \cdot \left(\sum_{t\geq 0} \frac{g_t}{t!} x^t \right) = \sum_{n,t\geq 0} \frac{c_n}{n!} \frac{g_t}{t!} x^{t+n}.$$

Observem que el coeficient de x^N amb N fix correspon a $\sum_{n+t=N} \frac{c_n}{n!} \frac{g_t}{t!}$ i per tant el coeficient de $\frac{x^N}{N!}$ és $N! \sum_{n+t=N} \frac{c_n}{n!} \frac{g_t}{t!} = \sum_{n=0}^{N} \left(\begin{array}{c} N \\ k \end{array} \right) c_k g_{N-k}$, i per tant el resultat. □

Exemple 2.40. *Considerem el problema de compteig on u_n sigui el nombre de permutacions amb repetició de longitud n d'un conjunt format per tres elements $\Omega := \{a, b, c\}$ on hi ha un número senar d'a's, un número parell de b's i sense restricció en c's. Considerem el producte de sèries formals:*

$$\Lambda := (\sum_{k\geq 0} 1 \cdot \frac{x^{2k+1}}{(2k+1)!}) \cdot (\sum_{i\geq 0} 1 \cdot \frac{x^{2i}}{(2i)!}) \cdot (\sum_{\ell\geq 0} 1 \cdot \frac{x^{\ell}}{(\ell)!})$$

i el coeficient $\frac{x^n}{n!}$ és exactament u_n, i per tant Λ és la funció generadora per a $(u_n)_n$ aquesta successió de nombres de compteig.

2.4 Equacions de recurrència lineal i funcions generadores

Definició 2.41. *Una successió $(u_n)_n$ de números en $\mathbb{K}$ satisfà una equació de recurrència lineal d'ordre k homogènia si compleix:*

$$u_n = a_1 u_{n-1} + \ldots + a_k u_{n-k} \tag{2.2}$$

per a tot $n \geq k$ amb k natural fixat per a certs elements de $\mathbb{K}$ $a_1, \ldots, a_k$ fixats.

Proposició 2.42. *Si tenim una successió $(u_n)_n$ satisfent (2.2) llavors la funció generadora $U(x) = \sum_{n\geq 0} u_n x^n$ és de la forma*

$$\frac{C(x)}{1 - a_1 x - \ldots - a_k x^k}$$

per a cert polinomi $C(x) \in \mathbb{K}[x]$ de grau com a molt $k-1$.

Demostració. Sigui $U(x) = \sum_{n\geq 0} u_n x^n \in \mathbb{K}[[x]]$ la funció generadora que busquem, on k és un natural ≥ 1 fixat. Observem primer que $x^k U(x) = \sum_{n\geq k} u_{n-k} x^n$.

Denotem per $U_N(x) := \sum_{i=0}^{N-1} u_n x^n \in \mathbb{K}[x]$ un polinomi de grau $N-1 \geq 0$ amb $N \geq 1$. Observem,

$$U(x)-U_k(x) = U(x)-(u_0+u_1x+\ldots+u_{k-1}x^{k-1}) = \sum_{n\geq k} u_n x^n = \sum_{n\geq k}(a_1u_{n-1}+\ldots+a_ku_{n-k})x^n =$$

$$a_1(\sum_{n\geq k} u_{n-1}x^n) + a_2(\sum_{n\geq k} u_{n-1}x^n) + \ldots + a_k(\sum_{n\geq k} u_{n-k}x^n) =$$

$$a_1x(U(x)-U_{k-1}(x)) + a_2x^2(U(x)-U_{k-2}(x)) + \ldots + a_kx^kU(x).$$

I per tant obtenim que

$$U(x)(1-a_1x-\ldots-a_kx^k) = U_k(x) - a_1xU_{k-1}(x) - \ldots - a_{k-1}x^{k-1}U_1(x)$$

on $C(x) = U_k(x) - a_1xU_{k-1}(x) - \ldots - a_{k-1}x^{k-1}U_1(x)$ és un polinomi de grau $\leq k-1$, determinats únivocament sabent $u_0, \ldots, u_{k-1}$ i $a_1, \ldots, a_{k-1}$. □

Exemple 2.43. *Considerem la successió de Fibonacci $(F_n)_n$ sota la relació homogènia lineal: $F_{n+2} = F_n + F_{n+1}$ per a $n \geq 0$. De*

$$F_n = (1)\cdot F_{n-1} + (1)\cdot F_{n-2}$$

tenim que $a_1 = a_2 = 1$ tenim llavors

$$\sum_{n\geq 0} F_n x^n = \frac{C(x)}{1-x-x^2}$$

on $C(x)$ és de grau com a molt 1 i per la demostració de la proposició igual a

$$C(x) = (F_0+F_1x) - 1x(F_0) = F_0 + x(-F_0+F_1).$$

Recordem que una successió $(a_n)_n$ ho podem pensar com $f \in \mathbb{N}^{\mathbb{K}}$ on A^B denota en aquest context aplicacions del conjunt A al conjunt B. Recordem del curs d'Àlgebra Lineal que $\mathbb{N}^{\mathbb{K}}$ és un $\mathbb{K}$-espai vectorial de dimensió no finita.

Denotem per

$$H_{a_1,\ldots,a_k}(\mathbb{K}) = \{f \in \mathbb{N}^{\mathbb{K}} | f(n) = a_1f(n-1) + \ldots + a_kf(n-k) \ \ \forall n \geq k\}$$

on $a_i \in \mathbb{K}$ números fixats on $a_k \neq 0$ d'ara en endavant sempre, o més en general denotem per

$$H_{h_1,\ldots,h_k}(\mathbb{K}) := \{f \in \mathbb{N}^{\mathbb{K}} | f(n) = h_1(n)f(n-1) + \ldots + h_k(n)f(n-k) \ \ \forall n \geq k\}$$

on $h_i \in \mathbb{N}^{\mathbb{K}}$ fixades (on aquí h_k no és l'aplicació zero).

Lema 2.44. *$H_{h_1,\ldots,h_k}(\mathbb{K})$ és un $\mathbb{K}$-subespai vectorial de $\mathbb{N}^{\mathbb{K}}$.*

Demostració. Siguin $f_1, f_2 \in H_{h_1,\ldots,h_k}(\mathbb{K})$, considerem $f_1+f_2 \in \mathbb{N}^{\mathbb{K}}$ i volem demostrar que aquesta aplicació f_1+f_2 pertany a $H_{h_1,\ldots,h_k}(\mathbb{K})$.

Observem que per $n \geq k$ tenim $(f_1+f_2)(n) = f_1(n)+f_2(n) = (\sum_{i=1}^k h_i(n)f_1(n-i))+(\sum_{i=1}^k h_i(n)f_2(n-i)) = \sum_{i=1}^k h_i(n)(f_1(n-i)+f_2(n-i)) = \sum_{i=1}^k h_i(n)(f_1+f_2)(n-i)$, i per tant $f_1+f_2 \in H_{h_1,\ldots,h_k}(\mathbb{K})$.

Ara considerem $f \in H_{h_1,\ldots,h_k}(\mathbb{K})$ i $\tilde{k} \in \mathbb{K}$ tenim $\tilde{k}\cdot f \in \mathbb{N}^{\mathbb{K}}$ i sol cal justificar que pertany a $H_{h_1,\ldots,h_k}(\mathbb{K})$ per a finalitzar.

Observem que per $n \geq k$ tenim $(\tilde{k}\cdot f)(n) = \tilde{k}f(n) = \tilde{k}(\sum_{i=1}^k h_i(n)f(n-i)) = \sum_{i=1}^k h_i(n)(\tilde{k}\cdot f)(n-i)$ i per tant el resultat.

□

Lema 2.45. *El subespai vectorial $H_{h_1,\ldots,h_k}(\mathbb{K})$ de $\mathbb{N}^{\mathbb{K}}$ té dimensió finita igual a k.*

Demostració. Exercici al lector. Deixem una indicació: considereu l'aplicació $\psi : H_{h_1,\ldots,h_k}(\mathbb{K}) \to \mathbb{K}^k$ definida per

$$\phi(f) = (f(0), f(1), \ldots, f(k-1)) \in \mathbb{K}^k$$

i demostreu que ϕ és una aplicació $\mathbb{K}$-lineal, injectiva i exhaustiva, per tant un isomorfisme d'espais vectorials i d'aquí obtingueu que la dimensió és igual a k. □

Una base per a $H_{h_1,\ldots,h_k}(\mathbb{K})$ podem triar $can_1, \ldots, can_k$ on $can_i(j) = \delta_{i-1,j}$ on $0 \leq j \leq k-1$ (la Delta de Dirac, que val zero llevat quan els dos subíndexs són el mateix on llavors val 1), fixeu-nos $can_1 \in H_{h_1,\ldots,h_k}(\mathbb{K})$ queda fixada un cop sabem

$$can_1(0) = 1, can_1(1) = 0, \ldots, can_1(k-1) = 0$$

ja que $can_i(n)$ amb $n \geq k$ queda determinada pels valors de $can_i(m)$ amb $m < n$ (els vectors can_i són vectors de $H_{h_1,\ldots,h_k}(\mathbb{K})$), per tant obtenim que

$$(can_1, \ldots, can_k)$$

forma una base per a $H_{h_1,\ldots,h_k}(\mathbb{K})$.

Qüestió 2.46. *Suposem ara que els coefficients són constant $a_1, \ldots, a_k$ enlloc de funcions $h_1, \ldots, h_k$. Podem trobar una base més fàcil per a $H_{a_1,\ldots,a_k}(\mathbb{K})$ que per exemple $(can_1, \ldots, can_k)$?*

Anem a respondreu-ho usant la funció generadora associada a $f \in H_{a_1,\ldots,a_k}(\mathbb{K})$ vista el dia anterior que era igual a $\frac{C(x)}{1-a_1x-\ldots-a_kx^k}$ on $C(x)$ és un polinomi de grau $k-1$ a coeficients en $\mathbb{K}$ fix un cop f és fixa.

Anem primer en aquest curs a expressar d'una altra manera (que l'obtinguda en la proposició anterior 2.42) la funció generadora per a successions recurrents homogènies complint (2.2). De la proposició 2.42 obtenim l'expressió

$$\frac{C(x)}{1 - a_1x - \ldots - a_kx^k}$$

on $C(x)$ té grau com a molt $k-1$. Escrivim $Q(x) = 1 - a_1x - \ldots - a_kx^k$

Definició 2.47. *Es defineix el* **polinomi característic** *per a qualsevol recurrència $(u_n)_{n\geq 0} \in H_{a_1,\ldots,a_k}(\mathbb{K})$ (és a dir complint (2.2)) al polinomi en t*

$$P(t) = t^kQ(1/t) = t^k - a_1t^{k-1} - \ldots - a_k \in \mathbb{K}[X]$$

Imposem d'ara en endavant **un cos $\mathbb{K}$ on $P(t)$ descomposa en factors lineals** i escrivim

$$P(t) = (t - \lambda_1)^{m_1} \cdot \ldots \cdot (t - \lambda_s)^{m_s}$$

on $\lambda_1, \ldots, \lambda_s \in \mathbb{K}$ les arrels de $P(t)$ i podem expressar la funció generadora:

$$U(x) = \frac{C(x)}{(1-\lambda_1x)^{m_1} \cdot \ldots \cdot (1-\lambda_sx)^{m_s}} =$$

$$\sum_{i=1}^{s} \left(\frac{c_{i,1}}{(1-\lambda_ix)} + \ldots + \frac{c_{i,m_i}}{(1-\lambda_ix)^{m_i}} \right) = \sum_{i=1}^{s} \sum_{j=1}^{m_i} \frac{c_{i,j}}{(1-\lambda_ix)^j}$$

amb $c_{i,j} \in \mathbb{K}$ constants.

Proposició 2.48. *Si tenim una successió $(u_n)_n$ en un cos $\mathbb{K}$ de característica zero satisfent (2.2) i el polinomi característic (de grau k) de la successió factoritza de forma lineal en $\mathbb{K}[x]$ mitjançant $\prod_{i=1}^{s}(x-\lambda_i)^{m_i}$[6]. Llavors existeixen k constants $c_{i,j} \in \mathbb{K}$ amb $1 \leq i \leq s$, $1 \leq j \leq m_s$ on podem escriure*

$$u_n = \sum_{i=1}^{s}\sum_{j=1}^{m_i} c_{i,j} \left(\begin{array}{c} n+j-1 \\ j-1 \end{array} \right) \lambda_i^n,$$

per a tot n. Igualment existeixen s polinomis $P_1(x), \ldots, P_s(x) \in \mathbb{K}[x]$ on cada $P_i(x)$ té grau com a molt $m_i - 1$ complint

$$u_n = \sum_{i=1}^{s} P_i(n)\lambda_i^n$$

per a tot $n \geq 0$.

Demostració. Abans hem demostrat que $\sum_{n\geq 0} u_n x^n = \sum_{i=1}^{s}\sum_{j=1}^{m_i} \frac{c_{i,j}}{(1-\lambda_i x)^j}$.

De l'exemple 2.37 tenim $\frac{c}{(1-x)^N} = c\cdot\left(\sum_{k\geq 0} \left(\begin{array}{c} N+k-1 \\ k \end{array} \right) x^k\right)$, amb $c \in \mathbb{K}$ constant. Per tant

$$\sum_{n\geq 0} u_n x^n = \sum_{i=1}^{s}\sum_{j=1}^{m_i} c_{i,j} \cdot \left(\sum_{k\geq 0} \left(\begin{array}{c} j+k-1 \\ k \end{array} \right) (\lambda_i x)^k \right),$$

ara comparant en la igualtat el terme de grau exactament x^n obtenim la igualtat:

$$u_n = \sum_{i=1}^{s}\sum_{j=1}^{m_i} c_{i,j} \left(\begin{array}{c} n+j-1 \\ j-1 \end{array} \right) \lambda_i^n.$$

Per la segona igualtat, sol hem d'observar que $P_i(n) := \sum_{j=1}^{m_s} c_{i,j} \left(\begin{array}{c} n+j-1 \\ j-1 \end{array} \right)$ és pot pensar com un polinomi $P_i(x)$ de grau com a molt $m_i - 1$ pensant que podem definir $\left(\begin{array}{c} x \\ t \end{array} \right) = \frac{x(x-1)\ldots(x-(t+1))}{t!}$ amb t natural.

□

Exemple 2.49. *Tornem a la successió de Fibonacci $(F_n)_{n\geq 0}$, tenim que el polinomi característic és*

$$P(t) = t^2 - t - 1 = (t - (\frac{1+\sqrt{5}}{2}))(t - (\frac{1-\sqrt{5}}{2}))$$

Tenim llavors $F_n = P_1(n)(\frac{1+\sqrt{5}}{2})^n + P_2(n)(\frac{1-\sqrt{5}}{2})^n$ on P_1, P_2 son polinomis de grau com a molt 0, és a dir constants e independents de n per tant

$$F_n = A(\frac{1+\sqrt{5}}{2})^n + B(\frac{1-\sqrt{5}}{2})^n$$

per a tot $n \geq 0$ on A, B constants.

[6]El cos $\mathbb{K}$ en ser de car. zero té sentit el polinomi $\left(\begin{array}{c} x \\ j \end{array} \right) := \frac{x(x-1)\ldots(x-(j+1))}{j!}$, és dir $j! \neq 0$ en $\mathbb{K}$.

Lema 2.50. *En la notació e hipòtesis de la proposició anterior, tenim que les funcions $f_{i,j} \in \mathbb{N}^{\mathbb{K}}$ complint*

$$f_{i,j}(n) = (n^j(\lambda_i)^n$$

amb $0 \leq j \leq m_i - 1$ e $1 \leq i \leq s$ compleixen que $f_{i,j} \in H_{a_1,\ldots,a_k}(\mathbb{K})$ i són vectors de $\mathbb{N}^{\mathbb{K}}$ linealment independents.

Demostració. De la demostració proposició anterior tenim que tot $f \in H_{a_1,\ldots,a_k}(\mathbb{K})$, existeixen constants $c_{i,j}$ i polinomis $P_i(x) = \sum_{j=0}^{m_i-1} c_{i,j}x^j$ de grau $m_i - 1$ complint que

$$f(n) = \sum_{i=1}^{s} P_i(n)\lambda_i^n = \sum_{i=1}^{s}\sum_{j=0}^{m_i-1} c_{i,j}(n^j\lambda_i^n)$$

per tant si fem $c_{i,j} = 1$ per cert valor concret de i i j, i zero altres constants tenim que f és combinació lineal dels $f_{i,j}$ i per tant

$$H_{a_1,\ldots,a_k}(\mathbb{K}) \subseteq \langle f_{i,j} | 1 \leq i \leq s, 0 \leq j \leq m_i - s\rangle = F$$

i com F és un s.e.v. de $\mathbb{N}^{\mathbb{R}}$ de dimensió màxima $k = \sum_{i=0}^{s}(m_i - 1)$, obtenim $F = H_{a_1,\ldots,a_k}(\mathbb{K})$ d'on $f_{i,j} \in H_{a_1,\ldots,a_k}(\mathbb{K})$ i en forma una base. □

Exemple 2.51. *Considerem la successions $H_{15,-84,208,-192}(\mathbb{R})$ tenim que el polinomi caracterıstic és:*

$$P(t) = t^4 - 15t^3 + 84t^2 - 208t + 192 = (t-3)\cdot(t-4)^3$$

per tant una base de $H_{15,-84,208,-192}(\mathbb{R})$ és:

$$((4^n)_n,\ (n4^n)_n,\ (n^24^n)_n,\ 3^n)$$

Ara si volem trobar $f \in H_{15,-84,208,-192}(\mathbb{R})$ complint que $f(0) = 1$, $f(1) = 2$, $f(2) = 0$ i $f(4) = 0$, hem de resoldre el sistema lineal:

$$f(n) = A(4)^n + Bn4^n + Cn^24^n + D3^n$$

on A,B,C, D constants on ha de ser vàlid per a tot n, en particular tenim

$$\begin{cases} A + 0 + 0 + D & = & f(0) = 1 \\ 4A + 4B + 4C + 3D & = & f(1) = 2 \\ 16A + 32B + 64C + 9D & = & f(2) = 0 \\ 64A + 192B + 576C + 27D & = & f(3) = 0 \end{cases}$$

i ens surt que $A = 33$, $B = -19/2$, $C = 1$ i $D = -32$ i per tant correspon al $f \in H_{15,-84,208,-192}(\mathbb{R})$ donat per $f(n) = -26\cdot 3^n - \frac{23}{3}\cdot n\cdot 3^n - \frac{5}{3}\cdot n^2\cdot 3^n + 27\cdot 4^n$.

Observació 2.52. *Fixeu-vos que $H_{a_1,\ldots,a_k}(\mathbb{K})$ sempre $a_k \neq 0$ ja que si fos zero no seria d'ordre k la relació, en particular el polinomi característic associat $P(t) = t^k - a_1t^{k-1} - \ldots - a_k$ no té l'arrel zero.*

Qüestió 2.53. *Com trobar una base de $H_{a_1,\ldots,a_k}(\mathbb{K})$ via successions relacionades amb les arrels del polinomi caracteristic associat a $H_{a_1,\ldots,a_k}(\mathbb{K})$, si aquest polinomi característic no factoritza en factors lineals en $\mathbb{K}[x]$?*

Exemple 2.54. *Considereu $H_{-1,-1}(\mathbb{R})$ que té dimensió 2, on $P(t) = t^2 + t + 1$ on les arrels són $\frac{-1+\sqrt{3}i}{2} = e^{\pm 2\pi i/3}$, i $P(t)$ és irreductible en $\mathbb{R}[t]$ i per tant no descomposa en factors de grau 1, en canvi si que ho fa en $\mathbb{C}$, observem que $\mathbb{C}$ és un $\mathbb{R}$-e.v. i la conjugació complexa σ té cos fix els nombres reals, pensant que un nombre complex podem escriure*

$$z = Re(z) + iIm(z) = \frac{z + \sigma(z)}{2} + i\frac{z - \sigma(z)}{2i}$$

on $Re(z) = \frac{z+\sigma(z)}{2}$ i $Im(z) = \frac{z-\sigma(z)}{2i}$ són reals obtenim que podem considerar com solucions de $H_{-1,-1}(\mathbb{R})$ les successions:

$$(\frac{-1+\sqrt{3}i}{2})^n + (\frac{-1-\sqrt{3}i}{2})^n = 2cos(n \cdot 2\pi/3);$$

$$(\frac{-1+\sqrt{3}i}{2})^n - (\frac{-1-\sqrt{3}i}{2})^n = 2isin(n \cdot 2\pi/3);$$

d'on obtenim que són linealment independents i per tant una base per a $H_{-1,-1}(\mathbb{R})$ és

$$(cos(n \cdot 2\pi/3))_n, sin(n \cdot 2\pi/3)_n).$$

En general per a $H_{a_1,\ldots,a_k}(\mathbb{K})$ on el polinomi caracteristic no factoritza en factors lineal en $\mathbb{K}[t]$, (pensem característica del cos $\mathbb{K} = 0$), llavors existeix un cos L que conté $\mathbb{K}$, on L és un K-espai vectorial de dimension finita igual a m, i exactament m automorfismes del cos L deixant fix K: $Aut_K(L)$, on les successions sobre L donades com potències de les arrels del polinomi caracteristic via certs automorfismes podem aconseguir elements de $H_{a_1,\ldots,a_k}(\mathbb{K})$, el cas més senzill on s'aplica aquesta idea és amb $\mathbb{K} = \mathbb{R}$, $L = \mathbb{C}$ i $Aut_{\mathbb{R}}(\mathbb{C})$ que està format per la conjugació complexa σ i l'automorfisme identitat.

En aquest curs no aprofundirem en buscar aquestes expressions per una base de $H_{a_1,\ldots,a_k}(\mathbb{K})$ quan $p(t)$ no factoritza en factors lineals en $\mathbb{K}[x]$.

Qüestió 2.55. *Què succeeix pel cas no homogeni i podem trobar-hi una funció generadora?*

Considerem $H_{a_1,\ldots,a_k;h}(\mathbb{K}) := \{f \in \mathbb{N}^{\mathbb{K}} | f(n) = a_1 f(n-1) + a_2 f(n-2) + \ldots + a_k f(n-k) + h(n), \forall n \geq k\}$, on $a_i \in \mathbb{K}$ fixades i $h \in \mathbb{N}^{\mathbb{K}}$.És facil demostrar que si $f_1, f_2 \in H_{a_1,\ldots,a_k;h}(\mathbb{K})$ llavors

$$f_1 - f_2 \in H_{a_1,\ldots,a_k}(\mathbb{K})$$

i per tant de ser no buit tenim que

$$H_{a_1,\ldots,a_k;h}(\mathbb{K}) = f + H_{a_1,\ldots,a_k}(\mathbb{K})$$

per a cert $f \in H_{a_1,\ldots,a_k;h}(\mathbb{K})$ i aquesta f és pot trobar provar funcions similars a $h(x)$, anem a fer-ne dos exemples on $h(x)$ està relacionat amb succession triant $\lambda = 1$. Per a aprofundir aquesta part podeu consultar [**?**].

Exemple 2.56. *Considerem $h(n) = 1$ per tot natural n, i considera $H_{2;h}(\mathbb{R}) := \{f \in \mathbb{N}^{\mathbb{R}} | f(n) = 2f(n-1)+1\}$ amb $f(0) = u_0$ (recordem que $H_2(\mathbb{R})$ té dimensió 1, i tota solució de $H_{2;h}$ serà una solució concreta de $H_{2;h}(\mathbb{R})$ sumada al e.v. $H_2(\mathbb{R})$). Anem a trobar-ne una funció generadora per a $f \in H_{2,h}$.*

Escrivim $U(x) = \sum_{k\geq 0} f(k)x^k$. *Observem*

$$\frac{U(x)-u_0}{x} = \sum_{j\geq 0} f(j+1)x^j = \sum_{j\geq 0}(2f(j)+1)x^j = 2(\sum_{j\geq 0} f(j)x^j)+(\sum_{j\geq 0} x^j) = 2\cdot U(x)+\frac{1}{1-x}.$$

Per tant tenim $\frac{U(x)-u_0}{x} = 2U(x) + \frac{1}{1-x}$, *d'aquí tenim* $U(x) - 2xU(x) = \frac{x}{1-x} + u_0 = \frac{x+u_0-u_0x}{1-x}$ *i per tant*

$$U(x) = \frac{x}{(1-x)(1-2x)} + u_0\frac{1}{x-2}$$

on $u_0\frac{1}{x-2}$ *és la funció generadora per a* H_2. *Observem que la funció* h *té a veure amb l'arrel 1 (veieu un lemma anterior) i és el factor* $\frac{1}{1-1x}$ *què apareix en buscar-ne una funció generadora concreta, aquest fet no és cap casualitat.*

Exemple 2.57. *Considerem* $h(n) = n-1$ *per tot natural* $n \geq 1$, *i considera* $H_{2;h}(\mathbb{R}) := \{f \in \mathbb{N}^{\mathbb{R}} | f(n) = 2f(n-1)+n-1 \forall n \geq 1\}$ *amb* $f(0) = u_0$ *(recordem que* $H_2(\mathbb{R})$ *té dimensió 1, i tota solució de* $H_{2;h}$ *serà una solució concreta de* $H_{2;h}(\mathbb{R})$ *sumada al e.v.* $H_2(\mathbb{R})$*) de dimensió 1. Anem a trobar una funció generadora per a* $f \in H_{2;h}$ *fixat.*

Escrivim $U(x) = \sum_{k\geq 0} f(k)x^k$. *Observem*

$$\frac{U(x)-u_0}{x} = \sum_{j\geq 0} f(j+1)x^j = \sum_{j\geq 0}(2f(j)+j)x^j = 2(\sum_{j\geq 0} f(j)x^j) + (\sum_{j\geq 0} jx^j).$$

A què correspon $\sum_{j\geq 0} jx^j$ *? fixem-nos és igual a* $x\cdot(\sum j \geq 0 \frac{d}{dx}(x^j))$ *i per tant formalment via la derivada formal igual a* $x\cdot\frac{d}{dx}(\sum_{j\geq 0} x^j) = x\cdot\frac{d}{dx}(\frac{1}{1-x}) = \frac{x}{(1-x)^2}$, *per tant obtenim*

$$\frac{U(x)-u_0}{x} = 2U(x) + \frac{x}{(1-x)^2}$$

on aquí obtenim

$$(1-2x)U(x) = \frac{x^2}{(1-x)^2} + u_0$$

i per tant

$$U(x) = \frac{x^2}{(1-x)^2(1-2x)} + \frac{u_0}{(1-2x)}$$

la funció generadora per a un $f \in H_{2;h}$.

Observem de nou que $u_0\frac{1}{x-2}$ *és la funció generadora per a* H_2. *Observem que la funció* h *té a veure amb l'arrel 1 i és el factor* $\frac{1}{1-1x}$ *què apareix en buscar-ne una funció generadora concreta on aquest* $h(n) = n1^n$ *apareix amb multiplicitat dos i veiem el factor* $(1-1x)^2$ *en el denominador en la funció generadora.*

Exemple 2.58. *Considerem* $h(n) = n$ *per tot natural* n, *i considera* $H_{0,1;h}(\mathbb{R}) := \{f \in \mathbb{N}^{\mathbb{R}} | f(n) = f(n-2)+n, \forall n \geq 2\}$ *amb* $f(0) = u_0$ *i* $f(1) = u_1$ *(recordem que* $H_{0,1}(\mathbb{R})$ *té dimensió 2, i tota solució de* $H_{0,1;h}$ *serà una solució concreta de* $H_{0,1;h}(\mathbb{R})$ *sumada al e.v.* $H_{0,1}(\mathbb{R})$*) de dimensió 1.*

Anem a trobar una funció generadora per a $f \in H_{0,1;h}$ *fixat.*

Escrivim $U(x) = \sum_{k\geq 0} f(k)x^k$. *Observem*

$$\frac{U(x) - u_0 - u_1 x}{x^2} = \sum_{j\geq 0} f(j+2)x^j = \sum_{j\geq 0}(f(j)+(j+2))x^j = (\sum_{j\geq 0} f(j)x^j)+(\sum_{j\geq 0} jx^j)+2(\sum_{j\geq 0} x^j).$$

Per tant $\frac{U(x)-u_0-u_1x}{x^2} = U(x) + \frac{x}{(1-x)^2} + 2\frac{1}{(1-x)}$ *i d'aquí s'obté:*

$$(1-x)(1+x)U(x) = (1-x^2)U(x) = u_0 + u_1 x + \frac{x^3}{(1-x)^2} + \frac{2x^2}{(1-x)}$$

i obtenim

$$U(x) = \frac{u_0 + u_1 x}{(1-x)(1-(-1)x)} + \frac{x^3}{(1-x)^3(1-(-1)x)} + \frac{2x^2}{(1-x)^2(1-(-1)x)}.$$

Capítol 3

Grafs

3.1 Primeres nocions de grafs simples

Definició 3.1. *Un graf simple és una parella $(\mathcal{V}, \mathcal{E})$ on $\mathcal{V}$ és un conjunt finit i $\mathcal{E}$ un subconjunt de $\mathcal{P}_2(\mathcal{V})$ on $\mathcal{P}_2(\mathcal{V})$ és el conjunt dels subconjunts de $\mathcal{V}$ format per 2 elements.*

Exemple 3.2. *Un graf simple correspon a $(\{1,2,3,4\}, \{\{1,3\},\{1,4\},\{1,2\},\{2,4\}\})$.*

Definició 3.3. *Donat $Gf = (\mathcal{V}, \mathcal{E})$ un graf simple:*

1. *el conjunt $\mathcal{V}$ s'anomena el conjunt de vertèxs per a Gf i s'anota $V(Gf)$, els elements de $V(Gf)$ s'anomenen vèrtexs.*

2. *el conjunt $\mathcal{E}$ s'anomena el conjunt de les arestes per a Gf i s'anota per $E(Gf)$, i els seus elements s'anomenen arestes on denotem per uv enlloc de l'aresta $\{u,v\}$. I un graf simple també el denotarem per $Gf = (V(Gf), E(Gf))$.*

3. *Dos vertexs u, v de G s'anomenen adjacents si $uv = \{u,v\} \in \mathcal{E}$, en aquests cas diem que u es troba en v. Diem u, v no adjacents si $uv \notin \mathcal{E}$.*

4. *Per a $v \in V(Gf)$, els veïns de v son els $u \in V(Gf)$ on $uv \in E(Gf)$.*

Un graf simple Gf el podem visualitzar sobre un pla, on dibuixem per cada vèrtex de Gf un punt, i cada aresta de Gf dibuixem una corba (linea usualment) unint els dos vèrtexs, on la posició dels punts i la forma del dibuix de les linies és lliure.

Exemple 3.4. *El graf anterior, $Gf = (\{1,2,3,4\}, \{\{1,3\},\{1,4\},\{1,2\},\{2,4\}\})$ una visualització és la següent:*

Exemple 3.5. *Anotem alguns grafs simples aquí tot fent-ne una visualització:*

1. *Donat $n \in \mathbb{N}$, considerem $Cop_n = (\mathcal{V}, \mathcal{E})$ on $\mathcal{V} = \{1, \ldots, n\}$ i $\mathcal{E} = \{\{u, v\} \in \mathcal{P}_2(\mathcal{V}) | mcd(u, v) = 1\}$. Observem que és un graf simple, i per exemple per $n = 6$ té una visualització:*

2. *El graf simple $(X, \mathcal{P}_2(X))$ on X un conjunt finit s'anomena complet i s'anota per K_X o també K_N on $N = |X|$. Visualitzem per exemple el graf complet K_3, correspon a:*

3. *El graf simple buit correspon a $(X, \emptyset)$ amb X un conjunt finit.*

Definició 3.6. *Sigui Gf un graf simple.*

1. *Un subconjunt $\{a, b, c\} \subset V(Gf)$ s'anomena un triangle de Gf si ab, bc i $ac \in E(Gf)$.*

2. *Un subconjunt $\{a, b, c\} \subset V(Gf)$ s'anomena un anti-triangle de Gf si ab, bc i $ac \notin E(Gf)$.*

Exemple 3.7. *Considerem el graf simple Cop_6, podeu observar que $\{1, 6, 5\}$ és un triangle de Cop_6.*

També podeu observar que $\{2, 4, 6\}$ és un anti-trinalge de Cop_6.

Proposició 3.8. *Sigui Gf un graf simple on $|V(Gf)| \geq 6$. Llavors una de les dues situacions següents succeeix:*

- *existeix un triangle en Gf,*
- *existeix un anti-triangle en Gf.*

Demostració. Triem $u \in V(Gf)$ (tenim almenys 5 vèrtexs diferents a u en Gf).

Cas 1: u té 3 veïns o més.

Sigui p, q, r veïns de u, si (o més d'un) pq,qr o $rp \in E(Gf)$ llavors Gf té un triangle (per exemple si $pq \in E(Gf)$ tenim $\{u, p, q\}$ és un triangle). Si cap pq,qr,rp és una aresta de Gf tenim que $\{p, q, r\}$ és un anti-triangle.

Cas 2: u té 2 o menys veïns. En particular el vèrtex u té 3 elements de $V(Gf)$ que no són veïns de u, anomenem-los: $\{p, q, r\}$. Si $pq, qr, pr \in E(Gf)$ obtenim que $\{p, q, r\}$ forma un triangle. Si algun $pq, qr, pr \notin E(Gf)$ tenim un anti-trianle (per exemple si $pq \notin E(Gf)$ llavors $\{u, p, q\}$ és un anti-triangle). □

Hi ha la següent generalització de l'anterior resultat que no demostrarem en aquest curs:

Fet 3.9. *Siguin N,M naturals positius. Sigui Gf un graf simple amb $|V(Gf)| \geq \binom{N+M-2}{M-1}$. Llavors, almenys una de les dues situacions següents succeeix:*

- *existeix N vèrtexs diferents de Gf que son mutuament adjacents (i.e. qualsevol dos d'aquests vèrtexs són adjacents),*
- *existeix M vèrtexs diferents de Gf que son mutuament no-adjacents (i.e. qualsevol dos d'aquests vèrtexs són no adjacents).*

Definició 3.10. *El número de Ramsey $R(N, M)$ és el natural més petit tal que tot graf amb $|V(Gf)| \geq R(N, M)$ llavors la conclusió de la proposició 3.9 és verifica.*

Exemple 3.11. *Considerem $R(3,3)$, de la proposició 3.9 tenim $R(3,3) \leq \binom{4}{2} = 6$.*

Considerem ara el graf simple de 5 vèrtexs:

$$Gf = (\{1,2,3,4,5\}, \{12, 23, 34, 45, 51\}).$$

És fàcil demostrar que no té cap triangle ni cap anti-triangle i per tant obtenim $R(3,3) = 6$. Exercici al lector escriure els detalls (podeu dir triangle o anti-triangle format vertexs senars ó 2 vertexs senar i 1 parell o bé 1 senar i 2 parells i veure que en cada situació no podem construir cap triangle ni cap anti-triangle).

Qüestió 3.12. *Calcular $R(N, M)$ explícitament? Més concretament $R(5,5)$?*

Definició 3.13. *Sigui Gf un graf simple, i $v \in V(Gf)$. El grau de v en Gf que anotem per $deg(v)$ o $deg_{Gf}(v)$ pel natural*

$$deg(v) := |\{e \in E(Gf) | v \in e\}|.$$

Clarament si Gf és un graf simple format per N vèrtexs i $v \in V(Gf)$ tenim $deg(v) \in \{0, 1, \ldots, N-1\}$

Proposició 3.14 (Encaixada de mans)**.** *Sigui Gf un graf simple, llavors*

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

Demostració. Considera $\mathcal{T} := \{(v, e) \in V(Gf) \times E(Gf) | v \in e\}$ i denotem $t = |\mathcal{T}|$.

- si fixem $v \in V(Gf)$ el nombre d'arestes on $(v, e) \in \mathcal{T}$ és exactament $deg(v)$. Per tant $t = \sum_{v \in V(Gf)} deg(v)$.
- si fixem $e \in E(Gf)$, aquest té exactament 2 vèrtexs, per tant $t = \sum_{e \in E(Gf)} 2 = 2 \cdot |E(Gf)|$.

□

Corol·lari 3.15. *Donat Gf un graf simple, llavors els nombre de vèrtexs v de Gf on $deg(v)$ és senar n'hi ha un nombre parell.*

Observació 3.16. *En teoria de grafs, la proposició (o millor lemma) de l'encaixada de mans afirma que cada graf simple té un nombre parell de vèrtexs de grau senar. El nom prové d'una versió més col·loquial del Corol.lari anterior 3.15 de la proposició (o lemma) 3.14: si algunes de les persones d'una trobada s'encaixen la mà en saludar-se, un nombre parell de persones haurà encaixat la mà amb un nombre senar d'altres. On una persona en la trobada ho representem per un vèrtex de Gf i fem una aresta entre un vèrtex a un altre si s'han encaixat la mà en saludar-se.*

Lema 3.17. *Donat Gf un graf simple amb $|V(Gf)| \geq 2$. Llavors existeixen $u, v \in V(Gf)$ amb $u \neq v$ on $deg(u) = deg(v)$.*

Demostració. Suposem l'oposat i arribem a contradicció. Sigui $N = |V(Gf)|$ i considerem l'aplicació $deg : V(Gf) \to \{0, \ldots, N-1\}$ on $v \mapsto deg(v)$. Si fos deg injectiva hi hauria un vertex de grau 0 i per tant sense cap veí, i un altre de grau $N-1$ i per tant tots els altres vèrtexs del graf hi són veïns, arribant a contradicció. □

Aquest resultat següent s'inclou en el que s'anomena "extremal graph theory":

Teorema 3.18 (Mantel)**.** *Sigui Gf un graf simple amb $N = |V(Gf)|$ i $e = |E(Gf)|$. Suposem que $e > N^2/4$. Llavors Gf té un triangle.*

Demostració. Observem que el cas $N = 3$ i $e \geq 3 > (9/4)$ sempre tenim un triangle. El cas $N = 4$ i $e \geq 5 > (4)^2/4$ també tot graf amb 4 vèrtexs i 5 arestes o més té un triangle (intenteu-ho formalitzar, exercici al lector).

Suposem cert l'enunciat per tots els grafs simples amb número de vèrtexs k amb $3 \leq k < N$ amb $e > k^2/4$ i provem-ho pels grafs simples amb exactament N vertèxs complint que el nombre d'arestes és $> N^2/4$.

Suposem que no hi hagués cap triangle. De $e > N^2/4 \geq 0$ tenim almenys una aresta $uw \in E(Gf)$.

Procedim de la següent manera, on pintem amb 3 colors les diferents arestes del graf Gf:

1. aresta uw de color negre,
2. cada aresta de Gf que conté el vertex u o w de color vermell,
3. altres arestes de color blau.

Observem que com a molt hi ha $N-2$ arestes vermelles, ja que cada vèrtex $v \in V(Gf) \setminus \{u, w\}$ (té $N-2$ vèrtexs $V(Gf) \setminus \{u, w\}$) pot conectar-se a u o a w però no ambdues (ja que suposem que no hi ha triangles i si es conectes a ambdues tindrien que vu, vw i uw formaria un triangle).

Considerem ara (V, S) on $V = V(Gf) \setminus \{u, w\}$ i S les arestes de color blau, i observem que és un graf simple, on no pot tenir cap triangle perquè Gf no tenia cap triangle, per tant

$$\#Arestes\ blaves \leq (N-2)^2/4$$

per hipòtesi d'inducció. On obtenim que el nombre d'arestes del graf Gf és

$$\leq 1 + (N-2) + \frac{(N-2)^2}{4} = \frac{N^2}{4}$$

on obtenim $e \leq N^2/4$ en contradicció. □

Observació 3.19. *En l'enunciat del teorema de Martel no podem debilitar les hipòtesis a* $e \geq \frac{N^2}{4}$. *Efectivament podem considerar el graf simple:*

$$Gf = (\{1,2,3,4,5,6\}, \{12,23,34,45,56,61,14,25,36\})$$

on no té cap triangle (cada costat de Gf *ajunta dos vertexs de paritat diferent, però un triangle necessariament tindrà dos vertexs amb la mateixa paritat), i observeu* $e = 9$ *i* $N = 6$ *on* $e = N^2/4$ *aquest graf sense cap triangle.*

Definició 3.20. *Sigui* Gf *un graf simple.*

- *un subgraf de* Gf *és un graf simple* Hf *on* $V(Hf) \subset V(Gf)$ *i* $E(Hf) \subset E(Gf)$.
- *Donat* $S \subseteq V(Gf)$ *un subconjunt, el subgraf de* Gf *induït per* S *és el subgraf* $(S, E(Gf) \cap \mathcal{P}_2(S))$.
- *Un subgraf* Hf *de* Gf *s'anomena induït si existeix un subconjunt* S *de* $V(Gf)$ *on* $Hf = (S, E(Gf) \cap \mathcal{P}_2(S))$.

Lema 3.21. *Sigui* Gf *un graf simple, i* Hf *un subgraf de* Gf. *Suposem que* Hf *és un graf complet, llavors* Hf *és un subgraf induït de* Gf.

Demostració. De ser Hf complet tenim $Hf = (V_1, \mathcal{P}_2(V_1))$ i de ser subgraf de Gf tenim $V_1 \subseteq V(Gf)$ i $\mathcal{P}_2(V_1) \subseteq E(Gf)$, per tant

$$Hf = (V_1, E(Gf) \cap \mathcal{P}_2(V_1))$$

és un graf induït. □

3.2 Isomorfisme de grafs

Definició 3.22. *Siguin* Gf_1, Gf_2 *dos grafs simples. Un isomorfisme de grafs entre* Gf_1 *a* Gf_2 *correspon a una bijecció* $\phi : V(Gf_1) \to V(Gf_2)$ *preservant les arestes, és a dir* $\forall u, v \in V(Gf_1)$ *tenim*

$$uv \in E(Gf_1) \Leftrightarrow \phi(u)\phi(v) \in E(Gf_2).$$

Diem que Gf_1 *i* Gf_2 *són grafs isomorfs (i escriurem* $Gf_1 \cong Gf_2$*) si existeix un isomorfisme de grafs entre ells.*

Exemple 3.23. *Considerem els grafs simples* $Gf_1 = (\{1,2,3,4,5,6\}, \{12,23,34,45,56,61\})$ *i* $Gf_2 = (\{1,2,3,A,B,C\}, \{1B,1C,2A,2C,3A,3B\})$. *Fer dibuix*

Definim $\phi : V(Gf_1) \to V(Gf_2)$ *bijectivament per* $\phi(1) = 1$, $\phi(2) = B$, $\phi(3) = 3$,$\phi(4) = A$,$\phi(5) = 2$ *i* $\phi(6) = C$, *afirmem que* ϕ *és un isomorfisme de*

grafs. Per això cal complir la condició que en les arestes ϕ s'aplica bijectivament, tenim 6 arestes a estudiar i per tant en aquest cas és factible fer-ho de forma ad-hoc, anem-ho a detallar:
Aresta $12 \in E(Gf_1)$ tenim $\phi(1)\phi(2) = 1B$ que efectivament es aresta de Gf_2 i viceversa.
Aresta $23 \in E(Gf_1)$ tenim $\phi(2)\phi(3) = 3B$ que és aresta de Gf_2 i viceversa
Aresta $34 \in E(Gf_1)$ tenim $\phi(3)\phi(4) = 3A$ que és aresta de Gf_2 i viceversa
Aresta $45 \in E(Gf_1)$ tenim $\phi(4)\phi(5) = 2A$ que és aresta de Gf_2 i viceversa
Aresta $56 \in E(Gf_1)$ tenim $\phi(5)\phi(6) = 2C$ que és aresta de Gf_2 i viceversa
Aresta $61 \in E(Gf_1)$ tenim $\phi(6)\phi(1) = 1C$ que és aresta de Gf_2 i viceversa
per tant ϕ porta bijectivament les arestes de Gf_1 a les arestes de Gf_2 i per tant obtenim que φ és un isomorfisme de Grafs i els grafs Gf_1 i Gf_2 són isomorfs.

Lema 3.24. *Sigui K_X el graf complet pel conjunt X d'N-elements, i escrivim K_N el graf complet pel conjunt $\{1, \ldots, N\}$. Llavors $K_X \cong K_N$.*

Demostració. Escrivint $X = \{a_1, \ldots, a_N\}$ i definint $\phi(a_i) = i$ obtenim un isomorfisme de grafs. □

Anem a llistar un conjunt de propietats de isomorfisme, molt senzilles de demostrar (tasca que deixem al lector).

1. donats Gf_1, Gf_2, Gf_3 tres grafs simples, si $Gf_1 \cong Gf_2$ i $Gf_2 \cong Gf_3$ llavors $Gf_1 \cong Gf_3$,
2. siguin Gf_1, Gf_2 dos grafs simples amb un isomorfisme de grafs entre ells, amb la bijecció $\phi : V(Gf_1) \to V(Gf_2)$, llavors
   (a) $\forall v \in V(Gf_1)$ tenim $deg_{Gf_1}(v_1) = deg_{Gf_2}(\phi(v_1))$
   (b) $|E(Gf_1)| = |E(Gf_2)|$, i $|V(Gf_1)| = |V(Gf_2)|$.
3. Donat Gf un graf simple i S un conjunt finit on $|S| = |V(Gf)|$, llavors existeix un graf simple Gf_2 isomorf a Gf on $V(Gf_2) = S$.

Definició 3.25. *Donat un graf simple Gf amb $|V(Gf)| = N$ on $V(Gf) = \{v_1, \ldots, v_N\}$ i fixem aquest ordre en el conjunt de vèrtexs!!!, llavors li associem la matriu adjacència $Adj(Gf) \in M_N(\mathbb{Z})$ definida*

$$(Adj(Gf))_{i,j} := \begin{cases} 1 & si \ \ v_i v_j \in E(Gf) \\ 0 & altrament \end{cases}$$

Exemple 3.26. *Considerem el graf simple $Gf = \{\{1,2,3,4,5,6\}, \{12, 23, 34, 45, 56, 61\}\}$ obtenim que té per matriu adjacència*

$$Adj(Gf) = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

Lema 3.27. *Sigui Gf un graf simple amb $V(Gf) = \{v_1, \ldots, v_N\}$ i fixem aquest ordre d'aquests elements i $Adj(Gf)$ matriu adjacència associada al graf. Llavors:*

1. *$Adj(Gf)$ és una matriu simètrica.*
2. *$Adj(Gf)_{i,i} = 0$,*
3. *el nombre de 1's en una fila o columna fixada i de la matriu $Adj(Gf)$ és el grau del vertex v_i.*

Demostració. Exercici al lector, fixeu-vos que $Adj(Gf)_{i,i} = 0$ perquè en la definició de graf simple no acceptem "loops" al voltant d'un vèrtex. □

Definició 3.28. *Una matriu $P \in M_n(\mathbb{Z})$ s'anomena de matriu de permutació si cada fila de P té una única posició que és $\neq 0$ i de valor 1, i cada columna de P té una única posició diferent de zero i de valor 1.*

Lema 3.29. *Una matriu P és de permutació si i només si s'obté de fer canvis elementals $F_i \leftrightarrow F_j$ i $C_i \leftrightarrow C_j$ a la matriu identitat de mida n.*

Demostració. Exercici al lector. □

Lema 3.30. *Sigui $P \in M_N(\mathbb{Z})$ una matriu de permutació, llavors P és invertible i $P^{-1} = P^t$.*

Demostració. Escrivim $(e_1, \ldots, e_N)$ amb e_i vector fila $1 \times N$ amb tot de zeros llevat a la possició i que té un 1.

Fixem-nos que donada $A \in M_n(\mathbb{Z})$ obtenim que $e_i A e_j^t = (A)_{i,j}$ el coeficient (i, j) de la matriu A.

Ara com P és una matriu de permutació compleix que $Pe_j^t = e_{\phi(j)}^t$ on ϕ és una bijecció del conjunt $\{1, \ldots, N\}$.

Amb les consideracions anteriors obtenim:

$$(P^t P)_{i,j} = e_i P^t P e_j^t = e_{\phi(i)} e_{\phi(j)}^t = \begin{cases} 1 & si\ \phi(j) = \phi(i) \\ 0 & altrament \end{cases}$$

per tant $P^t P = I_N$, d'on P és invertible amb inversa P^t. □

Proposició 3.31. *Dos grafs simples Gf_1 i Gf_2 són isomorfs si i només si existeix P una matriu de permutació on $Adj(Gf_1) = P^t Adj(Gf_2) P$.*

Demostració. Llistem en ordre els vèrtex de Gf_1: $(v_1, \ldots, v_N)$
Llistem en ordre els vèrtexs de Gf_2: $(w_1, \ldots, w_N)$.

Suposem primer que $Gf_1 \cong Gf_2$. Tenim $\phi : \{v_1, \ldots, v_N\} \to \{w_1, \ldots, w_N\}$ una bijecció entre $V(Gf_1)$ i $V(Gf_2)$ que dóna isomorfisme de grafs, i per tant tenim

$$(Adj(Gf_2))_{\phi'(i),\phi'(j)} = (Adj(Gf_1))_{i,j}$$

on $\phi'(i) = j$ prové de $\phi(v_i) = w_j$. Denotem per $(e_1, \ldots, e_N)$ les matrius $1 \times N$ on $e_1 = (1, 0, \ldots), \ldots, e_N = (0, \ldots, 0, 1)$ i podem identificar $(v_1, \ldots, v_N)$ amb $(e_1, \ldots, e_N)$ com també $(w_1, \ldots, w_N)$ amb $(e_1, \ldots, e_N)$ denotem per P la matriu de permutació on $Pe_i^t = e_{\phi'(i)}^t$.

Amb aquesta tria de matriu de permutació P obtenim:

$$(P^t(Adj(Gf_2)P)_{i,j} = e_i P^t(Adj(Gf_2))Pe_j^t = e_{\phi'(i)}Adj(Gf_2)e_{\phi'(j)}^t =$$
$$(Adj(Gf_2))_{\phi'(i),\phi'(j)} = (Adj(Gf_1))_{i,j}$$

per a tot $1 \leq i, j \leq N$, per tant obtenim que $P^t Adj(Gf_2)P = Adj(Gf_1)$.

Per la implicació contrària, si tenim aquesta P matriu de permutació tenim usant la notació anterior $Pe_i^t = e_{\phi'(i)}^t$ i dóna una bijecció $\phi : V(Gf_1) \to V(Gf_2)$ on $\phi(v_i) = w_{\phi'(i)}$ i és una comprovació que ϕ dóna un isomorfisme de grafs. □

Observació 3.32. *De la demostració anterior,* **llevat de conjugació per matrius de permutació** *"la" matriu adjacent a un graf Gf: $A(Gf)$ és independent de l'ordre que triem els vèrtexs, ja que en triar un altre ordre en $V(Gf)$, tenim que la matriu adjacent a Gf amb aquest nou ordre, diem-li $A(Gf)bis$ serà la conjugació per una matriu de permutació P on $P^t A(Gf)bisP = A(Gf)$.*

Definició 3.33. *Considerem un graf simple $Gf = (V(Gf), E(Gf))$.*

- *una seqüència de vertexs: $u_0, \ldots, u_\ell$ amb $u_{i-1}u_i \in E(Gf)$ per $1 \leq i \leq \ell$ s'anomena un* **recorregut** *R de longitud ℓ entre u_0 i u_ℓ del graf Gf.*
- *un* **circuit** *és un recorregut tancat, és dir amb $u_0 = u_\ell$ on no es repeteix cap aresta.*
- *quan tots els vèrtex d'un recorregut R són diferents diem que és un* **camí**, *i parlem de* **cicle** *quan és un camí tancat.*
- *Diem que el graf Gf és connex si $\forall u, v \in V(Gf)$ existeix un camí de u a v, i en aquest cas parlarem de distància entre u, v com la mínima longitud de camins entre u i v i s'anota $dist(u, v)$.*

Lema 3.34. *Sigui Gf un graf simple connex. Denotem per $D(Gf)$ al natural $max_{u,v\in V(Gf)}\{dist(u, v)\}$, i per cada $u \in V(Gf)$ l'excentricitat és el valor $e(u) := max_{v\in V(Gf)}\{dist(u, v)\}$ i definim $r(Gf) := min_{u\in V(Gf)}\{e(u)\}$. Llavors*

$$r(Gf) \leq D(Gf) \leq 2r(Gf).$$

Demostració. Clarament $r(Gf) = min_{u\in V(Gf)}e(u) \leq max_{u\in V(Gf)}e(u) = D(Gf)$. Ara si $u, v \in V(Gf)$ on $dis(u, v) = D(Gf)$ i sigui $w \in V(Gf)$ on $e(w) = r(Gf)$, tenim llavors

$$D(Gf) \leq dist(u, v) \leq dist(u, w) + dist(w, v) \leq e(w) + e(w) = 2r(Gf)$$

on hem usat que *dist* satisfà la desigualtat triangular(Exercici al lector). □

Proposició 3.35. *Sigui Gf un graf simple, i considerem la matriu adjunció amb graf amb l'ordre de vertex fixat per $(v_1, \ldots, v_N)$. Llavors $(Adj(Gf)^k)_{i,j}$ és el nombre de recorreguts de longitud k entre v_i i v_j (un walk indica una successió d'arestes $v_0v_1....v_\ell$ però les arestes i els vertexs es podrien repetit).*

Demostració. Escrivim $A = Adj(Gf)$ i demostrem-ho per inducció. Observem que $(A^k)_{i,j} = \sum_{\ell=1}^{N}(A^{k-1})_{i,\ell}A_{\ell,j}$, i tenim $(A^{k-1})_{i,\ell}A_{\ell,j}$ és no zero si $(A)_{\ell,j} = 1$ i $m = (A^{k-1})_{i,\ell} \geq 1$ on m són el nombre de recorreguts de longitud $k-1$ entre v_i a v_ℓ, per tant obtenim m recorreguts de v_i fins v_j on l'última aresta es $v_\ell v_j$, recorrent tots els vertèx v_ℓ obtenim el resultat. □

Qüestió 3.36. *Com decidir si dos grafs Gf_1 i Gf_2 són isomorfs a partir de $Adj(Gf_1)$ i $Adj(Gf_2)$?*

Sabem que són isomorfs si i només si hi ha una matriu P de permutació on

$$P^{-1}Adj(Gf_2)P = Adj(Gf_1)$$

i si comptem el número de matrius de permutació de mida $N = |V(Gf)|$ n'hi ha $N!$, donades dues matrius adjunció de mida N, és un problema computacional tant sols poder decidir si són isomorfes o no, lamentablement sembla que encara no és factible resoldre-ho d'aquesta manera, i anem a atacar-ho inicialment usant el curs d'Àlgebra Lineal del curs passat.

Si pensem $Adj(Gf)$ com una aplicació lineal en un cos $\mathbb{K}$ on $\{0,1\} \subset \mathbb{K}$, tenim per tota la teoria de classificació d'endomorfismes que tots els invariants d'endomorfismes associats a $Adj(Gf_1)$ i a $Adj(Gf_2)$ han de coincidir ja que és pase d'un a l'altre via un canvi de base P en el llenguatge d'Àlgebra Lineal, per tant obtenim el següent resultat conseqüència del curs d'Àlgebra Lineal (i com són matrius simètriques diagonalitzen com matrius a coeficients reals):

Lema 3.37. *Donat Gf_1 i Gf_2 dos grafs simples isomorfs, per a tot cos $\mathbb{K}$ on $\{0,1\} \subset \mathbb{K}$ llavors els polinomis característics en $\mathbb{K}[X]$ de les matrius adjunció coincideixen, també els polinomis mínims, en particular tindran els mateixos valors propis $\{\lambda_1, \ldots, \lambda_t\}$ pensant les matrius adjunció com matrius associades a una aplicació $\mathbb{K}$-lineal i $dim_{\mathbb{K}} Ker((Adj(Gf_1) - \lambda_j I_N)^k) = dim_{\mathbb{K}} Ker((Adj(Gf_2) - \lambda_j I_N)^k)$ per a tot $k \geq 1$ i λ_j un valor propi associat a $Adj(Gf_1)$ o $Adj(Gf_2)$ pensat com endomorfisme d'un $\mathbb{K}$-espai vectorial.*

Exemple 3.38. *Considerem els grafs $Gf_1 = (\{1,2,3,4\}, \{12, 23, 34, 41\})$ i $Gf_2 = (\{1,2,3,4\}, \{12, 13, 23, 34\})$, les matrius adjunció són les següents:*

$$Adj(Gf_1) = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix} \quad Adj(Gf_2) = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

tenim el polinomi característic associat a $Adj(Gf_1)$ és $p_{Adj(Gf_1)}(X) = X^4 - 4X^2$ i a $Adj(Gf_2)$ és $X^4 - 4X^2 - 2X + 1$, per tant Gf_1 no és isomorf a Gf_2. (hem fet els càlculs amb $\mathbb{K} = \mathbb{Q}$).

Exemple 3.39. *Sigui el graf $Gf_1 = \{\{1,2,3,4,5,6,7\}, \{17, 27, 37, 47, 57, 67\}\}$ i el graf $Gf_2 = \{\{1,2,3,4,5,6,7\}, \{34, 36, 37, 45, 56, 57\}\}$ que tenen per matrius adjuntes (amb ordre descrit pels vertexs) amb el mateix polinomi característic $x^5(x^2 - 6)$ [1]:*

$$Adj(Gf_1) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 \end{pmatrix} \quad Adj(Gf_2) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 \end{pmatrix}$$

[1] fixem-nos ambdues matrius adjuntes que presentem diagonalizen si pensem $\mathbb{K} = \mathbb{Q}$ o $\mathbb{R}$ i per tant subespais invariants no podrem descartar-les, però si fem a $\mathbb{K}$ igual $\mathbb{F}_2$ o $\mathbb{F}_3$ tenim llavors un únic valor propi

però clarament no podem construir un isomorfisme entre els grafs ja que un graf no té vèrtexs aïllats i l'altre sí.

3.3 Automorfisme d'un graf. Grafs amb automorfismes

Definició 3.40. *Un isomorfisme d'un graf (simple) Gf en ell mateix s'anomena automorfisme, en particular un automorfisme per a Gf és una permutació dels $V(Gf)$ que envia arestes a arestes i no-arestes a no-arestes. Al conjunt automorfisme d'un graf Gf l'anotarem $Aut(Gf)$.*

Observació 3.41. *$Aut(Gf)$ és un grup: fixem-nos id la permutació trivial en $V(Gf)$ és un automorfisme, i tot element de $Aut(Gf)$ correspon a una permutació de $V(Gf)$ per tant un subconjunt de $S_{V(Gf)}$, per veure és un grup, suficient veure és un subgrup de $S_{V(Gf)}$, i com clarament $id \in Aut(Gf)$ cal comprovar $\sigma_1, \sigma_2 \in Aut(Gf)$ llavors $\sigma_1 \circ \sigma_2 \in S_{V(Gf)}$ és també dins $Aut(Gf)$, però és clar per definició ja que σ_i envia arestes a aresta i per tant en la composició també, e igualment per no-arestes.*

Qüestió 3.42. *Com calcular $Aut(Gf)$ per a un graf (simple)?*

Amb matriu adjacència d'un graf és redueix amb un problema molt simple teòricament (computacionalment, en el moment actual no tant, del que conec).

Anem a observar-ho.

Observació 3.43. *No confonem automorfismes d'un graf amb diferents matrius d'adjunció d'un graf. Recordem que una matriu adjunció d'un graf, per a descriure-la cal fixar un ordre en els vèrtexs.*

Lema 3.44. *Les matrius de permutació de mida N és un grup que és isomorf a S_N al grup de permutacions d'N elements, (o al conjunt d'aplicacions bijectives del conjunt $\{1, \ldots, N\}$ en ell mateix).*

Demostració. Anem a demostrar que hi ha una bijecció φ entre $\mathcal{P}_N = \{P \in M_N(\mathbb{Z}) | P \text{ matriu de permutació}\}$ i S_N(aplicacions bijectives del conjunt $\{1, \ldots, N\}$). Construirem φ de manera que $\varphi(I_n) = id$ i $\varphi(P_1 \cdot P_2) = \varphi(P_1) \circ \varphi(P_2)$ on donarà isomorfisme de grups un cos demostrem que $\mathcal{P}_n$ amb el producte de matrius és un grup.

Denotem per $e_i = (0, \ldots, 0, 1, \ldots, 0)$ matriu fila tot de zero llevat posició $(1, i)$ té el valor 1. Prenem P una matriu de permutació. Tenim $Pe_i^t = e_{g(j)}^t$ per cert $g(j) \in \{1, \ldots, N\}$ i no poden coincidir ja que sol hi ha un valor diferent de zero en una columna i fila on g és un bijecció de $\{1, \ldots, N\}$ per i per tant definim $\varphi(P) = g$ d'una matriu permutació a una aplicació bijectiva de $\{1, \ldots, N\}$. A més $|\mathcal{P}_N| = N!$ (tenim N files i cal detallar en ordre posem 1's sense repetició en files) i $|S_N| = N!$ per tant si és injectiva o exhaustiva φ llavors ja serà bijectiva. Aquí podem observar que dos matrius de permutació P_1, P_2 diferents s'obté que $\varphi(P_1)$ és diferent de $\varphi(P_2)$ i per tant injectiva i concloem. (Una altra manera és construir aplicació inversa, ja que si tenim una bijecció f de $\{1, \ldots, N\}$ en ell mateix, fem columna i de P_f sigui exactament $e_{f(i)}^t$ obtenint així una matriu de permutació P_f on per construcció $\varphi(P_f)$ és f i per tant exhaustiva).

Ara veiem $\mathcal{P}_N$ és un grup amb el producte de matrius: $I_n \in \mathcal{P}_N$, i donada $P_1 \in \mathcal{P}_N$ existeix $P_2 \in \mathcal{P}_N$ on $P_1P_2 = P_2P_1 = I_N$ ($P_2 = P_1^t$), clarament serà associativa ja que el producte de matrius ho és, per tant sol falta justificar que el producte de dues matrius de permutació és de permutació, però com ambdues s'obtenen com aplicar iterativament canvis elementals de permutar dues files o dues columnes, el producte també s'obté a partir de la matriu identitat d'aquesta forma de com feiem el curs d''Algebra Lineal (ambdues matrius són productes de matrius elementals que sol involucren un canvi de files o un canvi de columnes), per tant s'obté que $\mathcal{P}_N$ és un grup.

Resta sol demostrar que $\varphi(P_1 \cdot P_2) = \varphi(P_1) \circ \varphi(P_2)$ (per veure φ a part d'una bijecció és un isomorfisme de grups). Escrivim $g = \varphi(P_1)$, $h = \varphi(P_2)$ i $t = \varphi(P_1P_2)$ com aplicacions bijectives del conjunt $\{1, \ldots, N\}$. Fixem-nos

$$e^t_{t(j)} = (P_1P_2)e^t_j = P_1(e_{h(j)})^t = e^t_{g(h(j))}$$

per tant $\varphi(P_1 \cdot P_2) = t = g \circ h = \varphi(P_1) \circ \varphi(P_2)$ i per tant concloem que φ és un isomorfisme de grups.

□

Definició 3.45. *Sigu Gf un graf simple i $A(Gf)$ matriu adjacent fixada amb un ordre dels vèrtexs fixat. Denotem per $\mathcal{M}(Gf)$ a les matrius de permutació de mida $|V(Gf)|$ complint*

$$A(Gf) = P^t A(Gf) P.$$

Lema 3.46. *Donat Gf un graf simple llavors $\mathcal{M}(Gf)$ és un subgrup de les matrius de permutació de mida $|V(Gf)|$.*

Demostració. Clarament $I_N \in \mathcal{M}(Gf)$, i si $P \in \mathcal{M}(Gf)$ fàcilment $P^{-1} \in \mathcal{M}(Gf)$ (pel Lemma 3.30). Siguin ara $P_1, P_2 \in \mathcal{M}(Gf)$, sol cal demostrar que $P_1P_2 \in \mathcal{M}(Gf)$. Efectivament,

$$(P_1P_2)A(Gf)(P_1P_2)^t = P_1(P_2A(Gf)P_2^{-1})P_1^{-1} = P_1A(Gf)P_1^{-1} = A(Gf).$$

□

Lema 3.47. *Hi ha un isomorfisme de grups entre $Aut(Gf)$ i $\mathcal{M}(Gf)$.*

Demostració. Anotem els vertexs de Gf amb l'ordre i notació $\{1, \ldots, N\}$ on així construïm $A(Gf)$, i com usual $e_j = (0, ..., 1, ...0)$ matriu fila amb únic element no zero en la columna j i de valor 1.

Sigui $\sigma \in Aut(Gf)$ en particular fa una permutació entre els vertèxs $\sigma(y) = l$ i definim P^t_σ on la columna y correspon a e^t_l,

$$(P_\sigma A(G) P^t_\sigma)_{i,j} = e_i P_\sigma A(G) P^t_\sigma e^t_j = A(G)_{\sigma(i),\sigma(j)}$$

com ara σ envia arestes a arestes i no-arestes a no-arestes tenim $A(G)_{\sigma(i),\sigma(j)} = A(G)_{i,j}$ (són 0,o 1's) i per tant $P_\sigma \in \mathcal{M}(Gf)$.

Això defineix una aplicació $\Lambda : Aut(Gf) \to \mathcal{M}(Gf)$ ($\sigma \mapsto P_\sigma$), on clarament $\Lambda(id) = I_{|V(Gf)|}$, i observem que amb la notació abans $\Lambda(\sigma_1 \circ \sigma_2) = P_{\sigma_1 \circ \sigma_2} = P_{\sigma_1}P_{\sigma_2} = \Lambda(\sigma_1)\Lambda(\sigma_2)$ per tant Λ és un morfisme de grups.

Falta demostrar que Λ és bijectiva. Construïm una aplicació inversa donada $P \in \mathcal{M}(Gf)$ escrivint $P^t e^t_i = e_j$, defineix σ_P una bijecció entre els vertexs de Gf

enviant vertex i al vertex j, com $PA(GF)P^t = A(Gf)$ obtenim que vèrtexs van a vèrtexs i no-vertexs a no-vertexs i per tant $\sigma_P \in Aut(Gf)$, definim $\Omega(P) = \sigma_P$. Per finalitzar cal veure que $\Lambda \circ \Omega = id_{\mathcal{M}(Gf)}$ i $\Omega \circ \Lambda = id_{Aut(Gf)}$, exercici al lector. □

Exemple 3.48. *El graf complet K_3, tota matriu de permutació dels vertexs porta arestes a arestes i no-arestes a no-arestes, per tant*

$$Aut(K_2) \cong \mathcal{P}_3 \cong S_3$$

Similarment en el graf complet K_N tota permutació dels vertexs dóna un isomorfisme, per tant $Aut(K_N) \cong S_N$.

Com calcular el grup automorfismes teòricament està resolt: cal comprovar fixada una matriu $A(Gf)$ i de les $N!$ matrius de permutació, calcular quines matrius de permutació deixen fixa la matriu $A(Gf)$ per conjugació. No obstant, a la pràctica aquest algoritme per calcular el grup d'automorfismes no es efectiu (quan N gran).

Qüestió 3.49. *Hi ha grafs sense automorfismes? Agafant un graf a l'atzar, esperem que tingui automorfismes?*

Tenim $Gf = (V(Gf), E(Gf))$ un graf on $N = |V(Gf)|$.

Lema 3.50. *El nombre de grafs (simples) diferents amb exactament $N \geq 2$ vertèxs són $2^{(N(N-1))/2}$.*

Demostració. En un graf simple amb N vertexs com a molt hi ha $\begin{pmatrix} N \\ 2 \end{pmatrix}$ arestes (correspon al nombre $\mathcal{P}_2(V(Gf))$), per tant per construir tots els grafs simples possibles cal decidir si una aresta l'agafem o no en aquesta construcció, per com tenim 2 possibilitats per aresta obtenim el resultat. □

Per abús notació escrivim $V(Gf) = \{1, \ldots, N\}$ i considerem el graf complet amb els N-vèrtexs $\{1, \ldots, N\}$ denotat per $K_N = (\{1, \ldots, N\}, \mathcal{P}_2(\{1, \ldots, N\}))$.

Siguin X, Y dos grafs (simples) amb N vertexs que els reanomenem el conjunt de vèrtexs de manera que el conjunt de vèrtexs per a X i per a Y és igual al conjunt $\{1, \ldots, N\}$ (d'ara en endavant en aquesta subsecció). Llavors podem pensar $E(X) \subset E(K_N)$ i $E(Y) \subset E(K_N)$. Donat $e = uv \in E(X)$ una aresta i $\sigma \in S_N$, llavors $\sigma(e)$ és l'aresta en K_N corresponent a $\sigma(u)\sigma(v)$.

Lema 3.51. *En la situació descrita en el paràgraf anterior: $X \cong Y$ si i només si $\exists \sigma \in S_N$ on $\sigma(E(X)) = E(Y)$.*

Demostració. Un isomorfisme entre X a Y ambdos grafs simples amb vèrtexs $\{1, \ldots, N\}$ és un $\sigma \in S_N$ que porta arestes a arestes (i no-arestes a no-arestes) i per tant $\sigma(E(X)) = E(Y)$, d'on el resultat. □

Considerem $t : S_N \times \mathcal{P}(E(K_N)) \to \mathcal{P}(E(K_N))$ on $\mathcal{P}(E(K_N))$ és el conjunt de les parts de les arestes del graf complet K_N, definit via $t(\sigma, X) := \sigma(X)$ on si $X = \{a_1, \ldots, a_s\}$ on a_j arestes en $E(K_N)$ amb vertexs $j_1, j_2 \in \{1, \ldots, N\}$ tenim $\sigma(X) = \{\sigma(a_1), \ldots, \sigma(a_s)\}$ on $\sigma(a_j)$ és aresta de $E(K_N)$ que correspon als vertexs $\sigma(j_1), \sigma(j_2)$.

Lema 3.52. *L'aplicació t defineix una acció (per l'esquerra) de S_N en $\mathcal{P}(E(K_N))$.*

Demostració. Tenim que clarament $t(id, X) = id(X) = X$. Considerem ara $t(\sigma_1 \circ \sigma_2, X) = \sigma_1 \circ \sigma_2(X) = \sigma_1(t(\sigma_2, X)) = t(\sigma_1, t(\sigma_2, X))$ i per tant defineix una acció. □

Fixem-nos que l'acció anterior defineix una relació:

Definició 3.53. *Siguin $U, V \subset E(K_N)$, diem $U \sim_t V$ si i només si existeix $\sigma \in S_N$ on $\sigma(U) = V$ o equivalentment $t(\sigma, U) = V$.*

Per tant pel Lemma 2.19 obtenim

Corol·lari 3.54. *La relació $\sim_t$ és una relació d'equivalència en $\mathcal{P}(E(K_N))$.*

Fixem-nos que donat un graf concret de N vertexs X podem pensar $E(X)$ un subconjunt de $E(K_N)$, i la clase de $E(X)$ via $\sim_t$ denotem per $[X] = \{\sigma(E(X)) | \sigma \in S_N\}$ que corresponen als grafs isomorfs a X pel Lemma 3.51 i vam demostrar dins el Lemma de Burnside:

$$|S_N| = |[X]| \cdot |(S_N)_X|$$

on $(S_N)_X := \{\sigma \in S_N | \sigma(E(X)) = E(X)\} = Aut(X)$ del Lemma 3.51, per tant

Lema 3.55. *Donat X un graf d'N-vertexs, el nombre de grafs isomorfs a X n'hi ha exactament $(N)!/|Aut(X)|$.*

Estudiem ara el conjunt quocient $|\mathcal{P}(E(K_N))/\sim_t|$ que correspon al nombre de classes d'isomorfismes de grafs amb exactament N vèrtexs. Pel Lemma de Burnside és igual a

$$\frac{1}{N!} \sum_{\sigma \in S_N} |(\mathcal{P}(E(K_N)))_\sigma|$$

Lema 3.56. *Tenim que $|(\mathcal{P}(E(K_N)))_\sigma| = 2^{ord(\sigma)}$ on $ord(\sigma)$ és el nombre de cicles disjunts de σ com un element de les permutacions en el conjunt de $\frac{N(N-1)}{2}$ elements: $E(K_N)$.*

Demostració. Pensem l'acció de σ en $E(K_N) := \{12, 13, \ldots, 1N, 23, 24, \ldots, 2N, \ldots, (N-1)N\}$ σ defineix una bijecció de $E(K_N)$ en ell mateix ($E(K_N)$ és d'un conjunt de $(N-1) + \ldots + 1 = \frac{N(N-1)}{2}$ elements) per tant podem pensar que σ és una permutació en $E(K_N)$ i la podem descriure com cicles disjunts

$$(\{12\}, \{\sigma(1)\sigma(2)\} \ldots, \{\sigma^{n_1}(1)\sigma^{n_1}(2)\})(\ldots)$$

Fixeu-vos que σ deixa invariant cada un d'aquests cicles, i agafant totes les arestes de un d'aquests cicles disjunt representa el subconjunts de $E(K_N)$, (un element de $\mathcal{P}(E(K_N))$) que deixa fix σ i el més petit subconjunt de $E(K_N)$ fix per σ que conte cada aresta dins el cicle.

Per tant podem formar tots els subconjunts de $E(K_N)$ invariants per σ fent unió d'aquests cicles disjunts, on el puc triar o no, per tant si tenim k cicles disjunts, obtenim 2^k possibilitats.

□

Exemple 3.57. *Pensem cas $N = 4$ i considerem el graf $Gf = (\{1, 2, 3, 4\}\{12, 23, 34, 41\})$ dins K_4. Calculem $[Gf]$ i quants elements té. Calculem $|(\mathcal{P}(E(K_4)))_\sigma|$ per alguns $\sigma \in S_4$ i $|\mathcal{P}(E(K_4))/\sim_t|$.*

- $[Gf] = \{\sigma(E(Gf))|\sigma \in S_4\}$, *aquest conjunt pot tenir* 24 *elements ja que* S_4 *té* 24 *elements. Fem-ne alguns exemples:*

$$\sigma = (12) \ \ tenim\sigma(E(Gf)) = \{12, 13, 34, 42\}$$

$$\sigma = (13) : \sigma(E(Gf)) = \{32, 21, 14, 43\} = E(Gf)(un\ automorfisme)$$

$$\sigma(24) : \sigma(E(Gf)) = \{14, 43, 32, 21\} = E(Gf)(un\ automorfisme)$$

$$\sigma = (123) : \sigma(E(Gf)) = \{23, 31, 14, 42\}$$

$$\sigma = (14) : \sigma(E(Gf)) = \{42, 23, 31, 14\}$$

Observem que $\sigma = (1234)$ *és un automorfisme ja que*

$$\sigma(E(Gf)) = \{23, 34, 41, 12\} = E(Gf)$$

per tant el sugbrup generat per (13),$(2, 4)$ *i* (1234) *(té ordre 8 almenys,* (1234) *genera grup ciclic ordre 4) està dins* $Aut(Gf)$ *i sabem* $|[Gf]| \cdot |Aut(Gf)| = |S_4| = 24$ *i per tant* $|[Gf]| \leq 3$ *i abans ja hem vist tres elements diferents per tant* $|[Gf] = 3$ *i és*

$$[Gf] = \{\{12, 23, 34, 41\}, \{12, 13, 34, 42\}, \{14, 23, 31, 42\}\}$$

i

$$Aut(Gf) = \{id, (13), (24), (1234), (13)(24), (1324),$$
$$(12)(34), (13)(1324), (24)(1234), (24)(1324)\}.$$

- *Calculem ara* $|(\mathcal{P}(E(K_4)))_\sigma|$ *per alguns* $\sigma \in S_4$.

  Fixem-nos primer que $E(K_4)$ *té* $3! = 6$ *elements:*

$$\{12, 13, 14, 23, 24, 34\} = \{A, B, C, D, E, F\}$$

  Si $\sigma = (13)$ *fixem-nos* $\sigma(A) = D$,$\sigma(B) = B$, $\sigma(C) = F$, $\sigma(D) = A$, $\sigma(E) = E$,$\sigma(F) = C$, *tenim doncs com cicles disjunts* $\sigma = (13)$ *com aplicació bijectiva en* $\{A, B, C, D, E, F\}$*:*

$$(A, D)(B)(C, F)(E)$$

  per tant tenim $|(\mathcal{P}(E(K_4)))_{(13)}| = 2^4$.

- *Calculem ara totes els grafs simples amb exactament 4 vertèxs mòdul isomorfisme que hi ha. Recordem que hi ha* 2^6 *grafs amb 4 vèrtexs. Hem de calcular* $\sum_{\sigma \in S_4} |(\mathcal{P}(E(K_4)))_\sigma|$, *i un càlcul s'obté (exercici al lector):*

$$|(\mathcal{P}(E(K_4)))_{id}| = 2^6; |(\mathcal{P}(E(K_4)))_{(a,b)}| = 2^4; |(\mathcal{P}(E(K_4)))_{(a,b)(c,d)}| = 2^4;$$

$$|(\mathcal{P}(E(K_4)))_{(a,b,c,d)}| = 2^2; |(\mathcal{P}(E(K_4)))_{(a,b,c)}| = 2^2$$

  on (a, b) *és un cile ordre 2 de* S_4 *(n'hi ha 6),* $(a, b)(c, d)$ *denota 2 cicles ordre 2 disjunts de* S_4 *(n'hi ha 3),* (a, b, c, d) *denota 4 cicle ordre exactament 4 de* S_4 *(n'hi ha 6), i* (a, b, c) *un cile ordre 3 (n'hi ha 8), per tant:*

$$|\mathcal{P}_2(E(K_4))/\sim_t| = \frac{1}{4!}(2^6 + 6 \cdot 2^4 + 3 \cdot 2^4 + 6 \cdot 2^2 + 8 \cdot 2^2) = \frac{264}{24} = 11.$$

  Per tant mòdul isomorfisme, sol hi ha 11 grafs simples no isomorfs formats exactament per 4 vèrtexs.

Observem que si tots els grafs d'N-vertexs fossin asimètrics (és a dir sense cap automorfisme) cada classe en $[X]$ tindria exactament $N!$ elements, per tant hauria de complir-se llavors que

$$|\mathcal{P}(E(K_N))/\sim_t| = (2^{(N(N-1))/2})/N!$$

però ja sabem que la classe de $[K_N]$ no en tindrà tants d'elements.

No obstant és pot demostrar:

Fet 3.58. *En la situació anterior s'obté que*

$$|(\mathcal{P}(E(K_N)))_\sigma| = (1+o(1))(2^{(N(N-1))/2})/N!$$

on $o(1)$ *significa que tendeix a 0 quan* $N \to +\infty$.

Per tant aquest fet que no demostrem, afirma que quan N gran quasi tots els grafs d'N-arestes no tindran automorfismes.

Qüestió 3.59. *Podeu construir un graf simple que no tingui automorfismes?*

Una construcció de grafs sense automorfismes explícits són els grafs de Halin per la persona interessada en aprofundir-hi.

3.4 Arc connex en grafs

Definició 3.60. *Sigui* Gf *un graf simple.*

1. *un recorregut (walk)* $u-v$ *de* Gf *de longitud* ℓ *on* $u,v \in V(Gf)$ *és* $(uu_1,\ldots,u_{\ell-1}u_\ell = u_{\ell-1}v)$ *on* $u_i \in V(Gf)$ *una familia ordenada de* ℓ *elements de* $E(Gf)$*, on comencem en el vertex* u *i finalitza en el vertex* v*. Parlem de recorregut obert si* $u \neq v$*, en cas contrari parlarem de recorregut tancat.*

2. *un senderó (trail) és un recorregut on no es repetix cap aresta.*

3. *un camí (path) és un recorregut on no es pot repeteix cap vèrtex de* Gf*.*

4. *un circuit és un senderó tancat.*

5. *un cicle és un circuit que té tots els vèrtexs diferents.*

Observació 3.61. *Un vèrtex* v *es considera un camí de longitud zero, i s'anomena camí trivial. Estenem la noció de longitud* ℓ *per senderons, camins, circuits i cicles, com també la noció de tancat i obert.*

Observació 3.62. *Un camí sempre és un senderó.*

Exemple 3.63. *Considera el graf complet* K_4*, tenim que* $\{13,34,41,12\}$ *és un recorregut de longitud* 4 *què és també un senderó, però no és un camí. Observem que* $\{12,23,34,41\}$ *és un cicle en* K_4*.*

Lema 3.64. *Sigui* $u,v \in V(Gf)$*. Aleshores tot recorregut* $u-v$ *conté un* $u-v$ *camí (és a dir un camí que s'inicia an* u *i finalitza en* v*)*

Demostració. Si $u - v$ no té cap vèrtex repetits ja és un camí.

Suposem doncs que $u - v$ té vèrtexs repetits. Escrivim el recorregut per $R : u = u_0 u_1 u_2 \dots u_\ell = v$ de longitud ℓ. Siguin i el natural més petit on $u_i = u_j$ amb $0 \leq i < j \leq \ell$. Suprimim a R la seqüència: $u_i u_{i+1} \dots u_j$ sol deixant el vèrtex $u_i = u_j$ obtenim el $u - v$ recorregut (de longitud més petita) donada per $R' : u_0 \dots u_i u_{j+1} \dots u_\ell$. Si tots els vèrtex de R' són tots diferents ja estem, altrament, iterem anterior procediment, i com el número de vèrtexs és finit en un recorregut obtenim que finalitzarem el procediment obtenint un $u - v$ camí (de longitud inferior usualment). □

Proposició 3.65. *Sigui Gf un graf simple, i considerem la matriu adjunció amb graf amb l'ordre de vertex fixat per $(v_1, \dots, v_N)$. Llavors $(Adj(Gf)^k)_{i,j}$ és el nombre de recorreguts de longitud k entre v_i i v_j (un walk indica una successió d'arestes $v_0 v_1 .... v_\ell$ però les arestes i els vertexs es podrien repetit).*

Demostració. Escrivim $A = Adj(Gf)$ i demostrem-ho per inducció. Observem que $(A^k)_{i,j} = \sum_{\ell=1}^{N} (A^{k-1})_{i,\ell} A_{\ell,j}$, i tenim $(A^{k-1})_{i,\ell} A_{\ell,j}$ és no zero si $(A)_{\ell,j} = 1$ i $m = (A^{k-1})_{i,\ell} \geq 1$ on m són el nombre de recorreguts de longitud $k-1$ entre v_i a v_ℓ, per tant obtenim m recorreguts de v_i fins v_j on l'última aresta es $v_\ell v_j$, recorrent tots els vertèx v_ℓ obtenim el resultat. □

Exemple 3.66. *Considerem el graf $Gf = (\{a, b, c, d\}, \{ab, ac, ad, bd, cd\})$ i tenim que amb ordre com hem escrit $Adj(Gf) = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$ obtenim $Adj(Gf)^2 = \begin{pmatrix} 3 & 1 & 1 & 2 \\ 1 & 2 & 2 & 1 \\ 1 & 2 & 2 & 1 \\ 2 & 1 & 1 & 3 \end{pmatrix}$ i $Adj(Gf)^3 = \begin{pmatrix} 4 & 5 & 5 & 5 \\ 5 & 2 & 2 & 5 \\ 5 & 2 & 2 & 5 \\ 5 & 5 & 5 & 4 \end{pmatrix}$ i per exemple $2 = (Adj(Gf))_{2,2}$ provenen dels recorreguts: bab, bdb, per exemple $5 = (Adj(Gf))_{2,1}$ són els recorreguts: abab, acab, adad, acdb, abdb.*

Definició 3.67. *Un graf Gf s'anomena connex* [2] *si $\forall u, v \in V(Gf)$ existeix un $u - v$ camí.*

Podem definir-ne una relació en $V(Gf)$: $u \sim_{ac} v \Leftrightarrow$ existeix un $u - v$ camí de Gf.

Lema 3.68. *La relació $\sim_{ac}$ és una relació d'equivalència en $V(Gf)$.*

Demostració. Reflexiva: tenim $u \sim_{ac} u$ ja que hem definit com el camí trivial de longitud 0 i per tant compleix aquesta propietat.
Simètrica: Si $u \sim_{ac} v$ tenim un $u - v$ camí, que també és un $v - u$ camí i per tant $v \sim_{ac} u$.
Transitiva: si $u \sim_{ac} v$ i $v \sim_{ac} w$ tenim un $u - v$ i un $v - w$ camí, ajuntant els dos camins tenim un $u - w$ recorregut en Gf i pel Lemma 3.64 obtenim un $u - w$ camí i per tant $u \sim_{ac} w$. □

Fixem-nos que Gf és connex (o arc-connex) si i nomes si $V(Gf)/\sim_{ac}$ està format per un sol element.

[2] Realment hauria de dir-se arc connex com veureu a topologia l'any vinent

Definició 3.69. *Donat Gf un graf $|V(Gf)/\sim_{ac}|$ s'anomena el nombre de components connexes del graf Gf. A la classe $[M] = \{a \in V(Gf) | a \sim_{ac} M\}$ associem el subgraf*

$$([M], E(Gf) \cap \mathcal{P}_2([M]))$$

que s'anomena la component connexa de Gf que conté $[M]$.

Qüestió 3.70. *Com decidir quant un graf Gf és connex o no?*

Hi ha algoritmes per donat un vertex $x \in V(Gf)$ trobar tots els elements de la classe $[x]$ en $V(Gf)/\sim_{ac}$ i per tant decidir si és connex o no. Un d'aquest algoritmes s'anomena algoritme DFS. No entrarem en detalls, però entenc que és un algoritme no exponencial i per tant factible a la pràctica en el moment actual i per tant decidir si es connex o no és un problema resolt des del punt de vista de l'enginyeria.

Anem a fer un petit resultat teòric que ha de complir un graf connex en aquest curs.

Lema 3.71. *Sigui Gf un graf connex on $N = |V(Gf)|$ i $M = |E(Gf)|$. Llavors $M \geq N - 1$.*

Demostració. Demostrem per inducció amb $N = |V(Gf)|$. Per $N = 1$ el resultat és clar. Suposem cert per a $N \leq k$. Sigui Gf un graf amb $|V(Gf)| = k + 1$ i $|E(Gf)| = M$. Volem demostrar que $M \geq k$. Anem a veure-ho:

a) si tots els vertexs de Gf compleixen que $deg(v) \geq 2$ amb $v \in V(Gf)$ llavors pel resultat de l'encaixada de mans Proposició 3.14 obtenim:

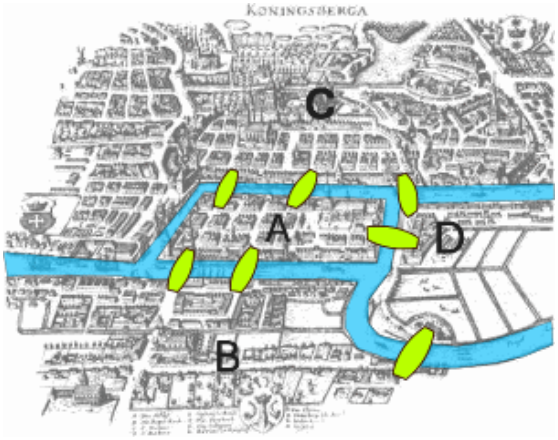
$$2M = 2|E(Gf)| = \sum_{v \in V(Gf)} deg(v) \geq 2(k+1)$$

i per tant obtenim que $M \geq k$ i ja estem.

b) de ser connex Gf no hi ha cap vèrtex $e \in V(Gf)$ amb $deg(v) = 0$. Ara si Gf té un vèrtex $v \in V(Gf)$ on $deg(v) = 1$ (diem a aquesta aresta $vu_0 \in E(Gf)$) considerem $Gf' := Gf \setminus v = \{V(Gf) \setminus \{v\}, E(Gf) \setminus \{vu_0\}\}$ que fàcilment es comprova que és connex (exercici al lector), i ara tenim $|V(Gf')| = k$ i $|E(Gf')| = M - 1$ per hipòtesi d'inducció obtenim que $M - 1 \geq k - 1$ i per tant en particular $M \geq k$, on el resultat. □

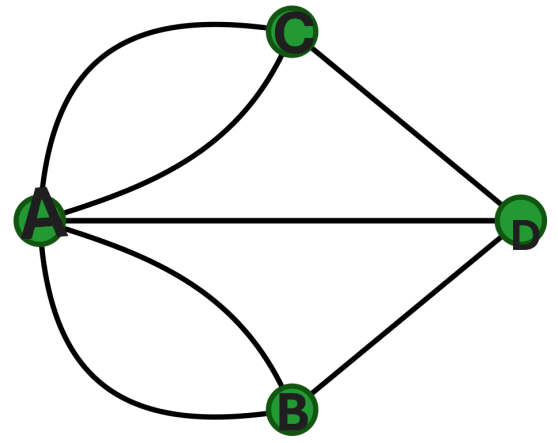
3.4.1 Grafs eulerians

Recordem el problema dels 7 ponts de l'antiga Königsberg (actualment Kaliningrad), que travessaven el riu Pregolya dins la ciutat. Era un joc entre els ciutadans si partint d'un lloc concret es podria fer un passeig per la ciutat de Königsbert atravessant els 7 ponts sense repetir-ne cap (on quan entrem per un pont no si val a mig camí tornar endarrera). Veieu-ne una representació:



Euler el 1736 transforma en problema en un graf i es comenta que aquesta resolució és l'inici de la teoria de grafs.

La idea és anomenar les diferents regions que separa el riu Pregolya amb:A,B,C,D com a vèrtex d'un grafs, i convertir els ponts en arestes del graf, fixem-nos que no surt un graf simple ja que entre els vèrtexs A i B hi tenim dos arestes, com també succeeix entre B i C.



Euler, observa que si no volem repetir camins passant pels ponts, quan arribem a un vertex per una aresta, hem de sortir del vertex per una altra aresta, i per tant per a poder fer el passeig per la ciutat de Königsberg sense repetir els ponts que atravessem cal que cada vèrtex del graf descrit tingui ordre parell, però ja veiem que $deg(C) = 3$ no parell per tant no és possible fer-ne el recorregut, i tancant Euler l'entreteniment que tenien els ciutadans de Königsberg. Anem a formalitar aquest problema en general.

Definició 3.72. *Si en un graf simple permetem l'existència d'arestes paral.leles, és a dir més d'una aresta entre un mateix parell de vèrtexs parlarem de multigraf. (Si a més admetem llaços (és a dir, una aresta d'un vèrtex a un mateix vèrtex) parlarem llavors de pseudografs).*

Observació 3.73. *El problema dels ponts de Königsberg es trasllada realment no en un graf simple sino en un multigraf.*

Definició 3.74. *Un senderó eulerià en un graf simple és un senderó no tancat que conté totes les arestes del graf. Un circuit eulerià en un graf simple és un*

circuit que conté totes les arestes del graf. Si un graf simple Gf conté un circuit eulerià direm que Gf és un graf eulerià.

Observació 3.75. *Podem estendre la noció de camins i senderons per a multigrafs, i en particular un multigraf Gf s'anomena eulerià si té un circuit que conté totes les arestes del graf (i.e. si té un circuit eulerià).*

Teorema 3.76 (Euler)**.** *Un graf (o multigraf) Gf és eulerià si i només si Gf és connex (llevat d'un número finit de vèrtexs aïllats, i.e. vertexs amb $deg(v) = 0$) i tots els vèrtexs no-aïllats de Gf tenen grau parell.*

Demostració. $\Rightarrow$ Si Gf té un circuit eulerià, tenim Gf connex llevat de tenir vertexs aillats. Considerem un circuit eulerià on s'inicia i finalitza en el vèrtex $v \in V(Gf)$ fixat. Per a $u \in V(Gf) \setminus \{v\}$ amb u no aïllat, cada vegada que el circuit arriba a u per una aresta ha de sortir-ne per una altra aresta (aresta no usada anteriorment), per tant $deg(u)$ ha de ser parell.

Ara considera v el vèrtex d'inici i final del circuit. Al nombre parell d'arestes quan v apareix durant el circuit cal afegir-hi l'aresta d'inici i l'aresta d'arribada, per tant també tenim $deg(v)$ és parell, finalitzant.

$\Leftarrow$ Es podem reduir a Gf connex i tot $v \in V(Gf)$ compleix $deg(v)$ és parell (si té vèrtexs aïllats es irredundant en buscar-hi un circuit eulerià). Partim d'un vèrtex $v_0 \in V(Gf)$ i construïm un recorregut C_0 sense cap aresta repetida (és a dir un senderó) de la forma següent: *donat $w \in V(Gf) \setminus \{v_0\}$, construïm un senderó de v_0 fins a w. Com $w \neq v_0$ hem usat un número senar d'arestes incidents amb w, i per tant com té grau parell podem continuar el senderó i arribem a fer un senderó de v_0 a un w_1, si aquest $w_1 \neq v_0$ podem iterar el procediment, i finalitza quan s'arriba a v_0 (i acaba ja que un nombre finit d'arestes). Per tant hem construït un circuit inicia v_0 i finalitza a v_0, diem-lo C_0 a aquest circuit. Si C_0 és eulerià, ja hem finalitzat.

En cas que C_0 no sigui un circuit eulerià, considerem H el graf (o multigraf) que s'obté de Gf en suprimir totes les arestes que hem usat en el circuit C_0. Fixem-nos que cada vèrtex d'H continua tenint grau parell (i els que surten de grau 0 els apartem ja que son vèrtexs aïllats i el circuit C_0 ja recorria en totes les arestes adjacents en aquests vèrtexs). Com C_0 no eulerià tenim un $v_1 \in V(H)$ amb $deg(v_1) > 0$ i que $v_1 \in C_0$ surt en el circuit C_0 (ja que si no existís aquest $v_1 \in C_0$ els vèrtexs amb arestes de H no tindrien camí amb els que es troben en el camí C_0 i això no es possible ja que Gf era connex), per tant tenim l'existència d'aquest v_1. Construïm a partir d'aquest $v_1 \in H$ un circuit C_1' dins H com hem fet en construir C_0. Ara com $v_1 \in C_0$ poden ajuntar els camins C_0 i C_1' en el punt v_1 obtenint un camí C_1 més llarg que conté més arestes de $E(Gf)$ totes no repetides. Ara si C_1 és un circuit eulerià finalitzem, en cas que no considerem H_1 sigui el graf de treure les arestes d'aquest circuit C_1 e iterant el procediment, com cada vegada el circuit C_i conté més arestes i tenim una finitud arestes arribem a construir un circuit eulerià. □

Observació 3.77. *Un Gf graf (o multigraf) connex és eulerià $\Leftrightarrow$ existeix una repartició del conjunt d'arestes de Gf en circuits.*

Definició 3.78. *Donat Gf un graf i $u, v \in V(Gf)$ no adjacents, $Gf + uv = (V(Gf), E(Gf) \cup \{uv\})$.*

Corol·lari 3.79. *Un graf (multigraf) Gf conté un senderó eulerià si i només si Gf és connex (llevat de possibles vèrtexs aïllats) i Gf té exactament 2 vèrtexs de grau senar.*

Demostració. $\Leftarrow$ Si Gf connex (llevat vertèxs aïllats) i sigui $u, v \in V(Gf)$ no aïllats amb grau senar. Considerem el graf $Gf + uv$ dels mateix vertexs que Gf però afegim l'aresta uv, observem que $Gf + uv$ continua sent connex (llevat de vèrtexs aïllats) i tots els vèrtexs de grau parell, per tant $Gf + uv$ té un circuit eulerià C (circuit que passe per l'aresta uv). Si treiem l'aresta uv en C obtenim un $u - v$-senderó en el graf Gf.

$\Rightarrow$ Exercici al lector. □

3.4.2 Grafs hamiltonians

Definició 3.80. *Un camí hamiltonià d'un graf (o multigraf) Gf és un camí que conté tots els vèrtexs de Gf. Un cicle hamiltonià d'un graf Gf és un cicle que conté tots els vèrtexs de Gf. Un graf hamiltonià és aquell que conté un cicle hamiltonià.*

Exemple 3.81. *El graf complet K_n és hamiltonià. Considerem* $12345 \ldots n1$ *és un cicle hamiltonià.*

El problema de trobar una "caracterització pràctica" per als grafs hamiltonians és un dels grans problemes oberts en la teoria de grafs, on es coneixen diverses condicions suficients perquè un graf Gf sigui hamiltonià, però cap és al mateix temps necessària.

Exemple 3.82. *K_3 és eulerià i hamiltonià. El graf $Gf1 = (\{1, 2, 3, 4, 5\}, \{12, 13, 23, 34, 35, 45\})$ és eulerià però no hamiltonià. El graf $Gf2 = (\{1, 2, 3, 4\}, \{12, 13, 23, 24, 34\})$ és hamiltonià i no eulerià. El graf $Gf3 = (\{1, 2\}, \{12\})$ és no eulerià i és no hamiltonià.*

És fàcil justificar (exercici al lector) que un graf Gf és hamiltonià, aleshores compleix les propietats següents:

1. Gf és connex i tots els seus vèrtex tenen grau ≥ 2. (És clar ja que un cicle hamiltonià recorre tots els vèrtexs, per tant donat dos vèrtexs hi ha el camí de quedar-nos en aquest cicle hamiltonià el camí entre aquests dos vèrtexs, i cada vèrtex té una aresta que arriba i una que surt d'haver-hi el cicle, per tant té cada vèrtex grau ≥ 2).

2. les arestes incidents en un vèrtex de grau exactament igual a 2 han d'aparèixer en tot cicle hamiltonià,

3. si estem construïnt un cicle hamiltonià, un cop hem visitat un vèrtex (hem entrat i sortit d'aquest vèrtex per dues arestes incidents amb ell) alehores podem suprimir totes les arestes restants que son incidents en aquest vèrtex.

4. un cicle hamiltonià no pot contenir un subcicle propi, és dir un cicle format per un conjunt més reduït de vèrtexs.

Exemple 3.83. *El graf* $Gf = (\{1,2,3,4,5,6,7,8,9\}, \{12, 23, 45, 56, 78, 89, 14, 47, 36, 69, 17, 39\})$ *no és hamiltonià, ja que si sortim el cicle hamiltonià en el vèrtex 2 no podem tornar-hi havent visitat (via les arestes de* Gf*) sol un cop els altres vèrtexs del graf* Gf*. Efectivament si iniciem el recorregut via* 2178 *no podem pasar pels vèrtexs 4 o 5, si* 21745 *no visitarem el vertex 8, si fem* 2145 *no visitarem 8 i per raons de simetria graf en dibuixar-ho podem concloure totes situacions no podem construir aquest cicle i per tant no és hamiltonià.*

Determinar si un graf és hamiltonià sembla un problema NP de computació, volen comentar que no hi ha cap algoritme conegut polinomial per aconseguir-ho en l'actualitat.

No obstant una idea general és: "si un graf té un nombre suficient d'arestes llavors el graf és hamiltonià".

Lema 3.84. *Sigui* Gf *un graf simple on* $N = |V(Gf)| \geq 3$ *i siguin* $u, v \in V(Gf)$ *no adjancents tals que* $deg(u) + deg(v) \geq N$*. Llavors*

$$Gf \text{ hamiltonià} \Leftrightarrow Gf + uv \text{ és hamiltonià.}$$

Demostració. És obvi que si Gf hamiltionià llavors $Gf + uv$ és hamiltonià.

Suposem que $Gf + uv$ és hamiltonià i C un cicle hamiltonià de $Gf + uv$. Si C no conté l'aresta uv ja és un cicle hamiltonià per a Gf i hem finalitzat.

Considerem doncs que C conté l'aresta uv. Llavors el recorregut de suprimir aquesta aresta en el cicle C obtenim un $u - v$ camí hamiltonià en Gf. Escrivim aquest camí per: $a_1 \dots a_t$ on $u = a_1$ i $v = a_t$. Demostrarem que hi ha un vèrtex a_{i+1} adjacent a u tal que a_i és adjacent a v, un cop vist això observem llavors que

$$a_1 a_{i+1} a_{i+2} \dots a_t a_i a_{i-1} \dots a_1$$

és un cicle hamiltonià de Gf i finaltizem (recomanem aquí fer-ne un dibuix $u = a_1 \dots a_i a_{i+1} \dots a_t = v$ dibuixant les arestes ua_{i+1} i va_i)

Anem a veure existència d'aquest vèrtex a_{i+1}. Suposem que no existís:

per a cada vèrtex del conjunt $\{a_2, \dots, a_N\}$ que fos adjacent a u hi hauria un vèrtex diferent del conjunt $\{a_1, \dots, a_{N-1}\}$ que no seria adjacent a v. Més detalladament si $deg(u) = d$ anomenem els vèrtexs adjacents a u per: $\{a_{i_1}, \dots, a_{i_d}\}$ amb $2 \leq i_1 < i_2 < \dots < i_d$, si no existís forçosament tenim que $a_{i_j - 1}$ haurien de ser no-adjacent a v, per tant $deg(v) \leq N - 1 - d$. Aleshores si $deg(u) = d$ tenim que $deg(v) \leq N - 1 - d$ i per tant $deg(u) + deg(v) \leq N - 1$, en contra hipòtesi, per tant existeix aquest vèrtex. □

Teorema 3.85 (Ore, 1961)**.** *Si* Gf *és un graf simple amb* $N = |V(Gf)| \geq 3$*, tal que per a tot parell de* $u, v \in V(Gf)$ *no adjacents de* Gf *es compleix que* $deg(u) + deg(v) \geq N$ *llavors* Gf *és hamiltonià.*

Demostració. Si en el graf Gf afegim una aresta uv on u i v no adjacents, per la hipòtesi i pel teorema anterior obtenim que Gf hamiltonià si i només si $Gf + uv$ és hamiltonià. Per tant la propietat de ser hamiltonià o no, tenim que no s'altera en afegir a Gf arestes de vèrtexs no adjacents. Afegint-hi totes aquestes arestes obtenim el graf complet K_N que en ser K_N hamiltonià, obtenim que Gf és un graf hamiltonià. □

Corol·lari 3.86 (Dirac, 1952)**.** *Si* Gf *és un graf simple amb* $N = |V(Gf)| \geq 3$ *i per a tot* $u \in V(Gf)$ *compleix* $deg(u) \geq \frac{N}{2}$*, llavors* Gf *és un graf hamiltonià.*

3.5 Conceptes bàsics d'arbres

Definició 3.87. *Un arbre és un graf connex sense cicles (diem acíclic a un graf sense cicles).*

Lema 3.88. *Donat un graf simple Gf, són equivalents:*

i) Gf *és un arbre,*

ii) entre cada parell de vèrtexs de Gf *existeix un únic camí,*

iii) Gf *és connex, complint* $|E(Gf)| + 1 = |V(Gf)|$.

iv) Gf *és acíclic però* $Gf + uv$ *conté un cicle per a tot* $u, v \in V(Gf)$ *on* u, v *no adjacents.*

v) Gf *és connex però* $Gf \setminus e = (V(Gf), E(Gf) \setminus e)$ *és no connex per a tota* $e \in E(Gf)$.

Demostració. i) $\Rightarrow$ *ii)*: existeix el camí per a ser Gf connex. Si tenim dos camins C_1, C_2, tenim dos $u-v$ recorreguts, ajuntant els dos recorreguts obtenim un $u-u$-recorregut no-trivial i amb un argument similar al Lema 3.64 obtenim que conté un cicle no-trivial, i no és possible per ser Gf un arbre.
ii) $\Rightarrow$ *i)*: com per cada dos vèrtexs hi ha un camí obtenim que Gf és connex. Falta sol justificar que Gf és acíclic: si té un cicle no trivial, hi hauria dos camins per cada dos vèrtexs del cicle, per tant és acíclic.
i) $\Rightarrow$ *iii)*: Fem inducció respecte al número de vèrtexs. Si Gf té 1,2 o 3 vèrtexs és clar tots els arbres possibles i compleixen $|E(Gf)|+1 = |V(Gf)|$ (recomanem al lector dibuixar aquests arbres per aquest nombre de vèrtexs).

Hipòtesi d'inducció: Tot arbre Gf on $|V(Gf)| \leq N$ llavors $|E(Gf)| + 1 = |V(Gf)|$.

Agafem un arbre Gf amb $|V(Gf)| = N + 1$ i triem $e = uv \in E(Gf)$. El camí de l'arbre entre les arestes u i v és únic i és uv, per tant si considerem el graf $Gf \setminus \{uv\} = (V(Gf), E(Gf) \setminus \{uv\})$ es separa en dos components connexes T_u i T_v i com Gf acíclic, també ho és T_u i T_v per tant T_u i T_v són arbres, i $|V(T_1)| = k_1 \leq N$ i $|V(T_2)| = k_2 \leq N$, i per tant per hipòtesi inducció $|E(T_1)| = k_1 - 1$ i $|E(T_2)| = k_2 - 1$ i per tant

$$|E(Gf)| = (k_1 - 1) + (k_2 - 1) + 1$$

i com $|V(Gf)| = N = k_1 + k_2$ per construcció de T_1 i T_2, obtenim el resultat.

iii) $\Rightarrow$ *i)*: Per hipòtesi inducció amb el nombre de vèrtexs, on si aquest nombre és 1 o 2 és clar. Considerem Gf un graf connex amb $N+1$ vèrtexs i N arestes i volem veure és un arbre.

Donat $u \in V(Gf)$ amb $deg(u) = 1$ (efectivament, de ser conex $deg(v) \geq 1$ per a tot vertex, si tots complissin que $deg(v) \geq 2$ pel lema d'encaixades de mans tenim $2N = 2deg(v) \geq \sum_{v \in V(Gf)} deg(v) = 2(N + 1)$ i no és possible), i considera el graf $Gf \setminus u = (V(Gf) \setminus u, E(Gf) \setminus \{uu_0\})$ on uu_0 és l'única aresta incident amb vèrtex u (de tenir grau 1). Observem que $Gf' = Gf \setminus u$ és connex i $|V(Gf')| = N$ i $|E(Gf')| = N-1$ i per tant Gf' és un arbre, i clarament afegir aresta uu_0 continua sent acíclic i per tant un arbre.

iv) $\Leftrightarrow$ *i)* Exercici al lector. *v)* $\Leftrightarrow$ *i)*: exercici al lector. $\square$

Definició 3.89. *Donat un graf Gf un subgraf de Gf és $H = (V, E)$ on $V \subseteq V(Gf)$ i $E \subseteq E(Gf) \cap \mathcal{P}_2(V)$.*

Definició 3.90. *Un arbre generador d'un graf Gf és un subgraf T de Gf on $T = (V(T), E(T))$ és un arbre complint que $V(T) = V(Gf)$.*

Lema 3.91. *Tot graf connex Gf té un arbre generador.*

Demostració. Si Gf és un arbre, ja estem, altrament Gf té un circuit, diem-lo C. Si fem $Gf_1 = (V(Gf), E(Gf) \setminus e)$ amb $e \in C$ una aresta del circuit, tenim que Gf_1 continua sent connex i amb una aresta menys que Gf. Si Gf_1 és un arbre ja estem, altrament conté un circuit, diem-lo C_1, triant una aresta e_1 d'aquest circuit C_1 obtenim un subgraf de Gf connex amb una aresta menys: $Gf_2(V(Gf), E(Gf_1) \setminus e_1)$, si és aciclic, ja estem, altrament té un circuit e iterant el procediment anterior i com tenim un nombre finit d'arestes, hi haurà un moment que finalitzem. □

Qüestió 3.92. *Quants arbres generadors hi ha en un graf connex Gf?*

Exercici 3.93. *Expliciteu arbres generadors per a K_2, K_3 i K_4.*

Definició 3.94. *Sigui $Gf = (\{a_1, \ldots, a_N\}, \{e_1, \ldots, e_M\})$ un graf simple (o multigraf). Triem aquest ordre en els vèrtexs i les arestes del graf, i definim la matriu d'incidència a la matriu de mida $N \times M$ denotada per $In(Gf) \in M_{N,M}(\mathbb{Z})$ definida per*

$$(In(G))_{i,j} = \left\{ \begin{array}{cc} 1 & \text{si } a_i \text{ incident en } e_j \\ 0 & \text{altrament} \end{array} \right\};$$

Exemple 3.95. *Considera el graf $Gf = (\{1, 2, 3, 4\}, \{12, 13, 14, 34\})$, tenim amb aquest ordre que*

$$In(Gf) = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

Definició 3.96. *Una matriu incidència reduïda pel graf Gf correspon a fixar un vèrtex de referència en un graf i eliminar la fila de la matriu $In(Gf)$ corresponent a aquest vèrtex fix. Si volem fer explicit el vèrtex eliminat v la podem descriure aquesta matriu com $In(Gf)_{kill:v}$ o $In(Gf)_v$.*

Exemple 3.97. *Continuem amb l'exemple 3.95, i fixem el vèrtex 4 com a referència, llavors tenim*

$$In(Gf)_4 = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}.$$

Definició 3.98. *Anomenem matriu reduïda associada a un digraf de Gf on fixem un vèrtex v de Gf a una matriu que s'obté de $In(Gf)_{kill:v}$ canviant exactament un 1 en cada columna d'aquesta matriu per un -1, denotem aquestes matrius per $InDi(Gf)_{kill:v}$.*

Si H és un subgraf de Gf on $V(H) = V(Gf)$ amb $|V(Gf)| = N$ i $|E(H)| = N - 1$, tenim $InDi(Gf)_v \in M_{N-1 \times M}(\mathbb{Z})$ amb $M \geq N - 1$. Si ens restrigim a les columnes de $InDi(Gf)_v$ corresponent al subgraf H obtenim una matriu quadrada de mida $N - 1$ que denotem per $InDi(Gf)_{v,H}$.

Lema 3.99. *Donat Gf un graf, i H un subgraf amb $V(Gf) = V(H)$ on H té $N-1$ arestes, llavors el valor absolut del determinant de la matriu $InDi(Gf)_{v,H}$ no depen del v triat i de l'elecció de -1's triat per a obtenir la matriu reduïda associada al digraf de Gf, i anotem $|det(InDi(Gf)_{v,H})|$ per $|det(In(Gf)_H)|$.*

Demostració. Exercici al lector. Indicació: considereu en la matriu $In(Gf)$ la fila F_v corresponent al vèrtex v i F_u la corresponent a un altre vèrtex u, i en cada columna de $In(Gf)$ on hi ha exactament dos 1's, canviem un d'aquests 1's per un -1, podem dir a aquesta matriu $InDi(Gf)$. Considerem B la matriu que s'obté de $InDi(Gf)$ treiem la fila F_u i F_v amb els signes 1 i -1 que haguem posat i denotem per C la matriu $\left(\frac{B}{F_u+F_v}\right)$, i d'aquesta matriu $N-1 \times M$ considerem la submatriu $N-1 \times N-1$ agafant les columnes corresponent a H i té determinant 0, (les suma de les seves files és la fila zero), i desenvolupant per l'última fila de la submatriu d'$N-1$-columnes de C s'obte $|det(InDi(Gf)_{u,H})| = |det(InDi(Gf)_{v,H})|$, on la tria 1 o -1 en una columna no afecta en tot el procediment ja que el valor absolut del determinant continua essent el mateix (correspon a l'operació de multiplicar per -1 una columna i per tant el valor absolut del determinant no varia). □

Exemple 3.100. *Continuant amb l'exemple 3.95 triem el subgrap de Gf $H = (\{1,2,3,4\},\{12,13,14\})$, obtenim que $InDi(Gf)_4 = \begin{pmatrix} -1 & -1 & -1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix}$ i $In(GfDj)_{4,H} = \begin{pmatrix} -1 & -1 & -1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$. Fixem-nos que una altra elecció en 1 i -1's seria $InDi(Gf)_4 b = \begin{pmatrix} 1 & -1 & -1 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix}$ i $In(GfDj)_{4b,H} = \begin{pmatrix} 1 & -1 & -1 \\ -1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$ i observem que $|det(In(GfDj)_{4,H})| = |det(In(GfDj)_{4b,H})| = 1$.*

Si canviem el vèrtex de referència en la reduïda observem per exemple que $In(Gf)_3 = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$, i per tant una $InDi(Gf)_3 = \begin{pmatrix} -1 & -1 & -1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 \end{pmatrix}$ i $InDi(Gf)_{3,H} = \begin{pmatrix} -1 & -1 & -1 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ que té el valor absolut del determinant valor igual a 1.

Proposició 3.101. *Un subgraf T d'un graf simple connex Gf amb $V(T) = V(Gf)$ és un arbre generador de Gf si i només si $|det(InDi(Gf)_T)| = 1$.*

Demostració. Sigui T un arbre generador de Gf, per tant $|V(T)| = |V(Gf)| = N$ i $|E(T)| = N-1$. Del lema d'encaixada de mans sabem $\sum_{v \in V(T)} deg(v) = 2N-2$ i per tant T té almenys dos vèrtexs u de grau 1. Triem un vèrtex de referència v_r i un vèrtex $u_1 \neq v_r$ on $deg(u_1) = 1$ i denotem per b_1 aresta de T on el vèrtex u_1 hi és incident. Iterem el procediment i triem vèrtex u_i amb $i = 2,\ldots,N-1$ amb $u_i \neq v_r$ que tingui grau 1 en l'arbre $T \setminus \{u_1,\ldots,u_{i-1}\}$ i triem b_i aresta on aquest u_i hi incideix. Fixem-nos que amb aquesta elecció d'ordre d'arestes $b_1,\ldots,b_{N-1}$ i vèrtexs $\{u_1,\ldots,u_{N-1}\}$ la matriu incidència és

triangular on en la diagonal hi ha 1's o -1's i per tant té determinant zero (recordo que un canvi de files o columnes no canvia el valor del determinant).

Suposem ara que tenim H un subgraf de Gf amb $V(H) = V(Gf)$ i amb $|E(H)| = N-1$ però H no sigui un arbre, això vol dir que H és no connex o si ho és (seria un graf) però no un arbre generador, estudiem que succeeix amb el determinant aquestes dues situacions.

Si H no és connex: siguin els vertexs $u_1, \ldots, u_t$ que pertanyen a la component connexa que no conté el vector v_r i siguin $b_1, \ldots, b_s$ les arestes contingudes en la component connexa que no conté el vector v_r, i triem aquesta ordenació en la matriu incidència $In(Gf)_{v_r}$: $\{u_1, \ldots, u_t, u_{t+1}, \ldots, u_{N-1}\}$ i $\{b_1, \ldots, b_s, b_{s+1}, \ldots b_{N-1}\}$ per tant si fem

$$(1 \ldots^t 1|0 \ldots |0) InDi(Gf)_{v_r,H} = (0 \ldots 0)$$

perquè les primeres t columnes tenen 1 i -1 de la fila 1 a la fila t per ser de la component connexa que no conté v_r i per tant obtenim $det(InDi(Gf)_{v_r,H}) = 0$.

Si H és connex (però no arbre generador de Gf): tenim que afegint una aresta de Gf en H seria un arbre (cosa impossible per la caracterització d'arestes i vèrtexs d'un grafs) o tindria un cicle (això imposaria que H realment és un arbre generador per a Gf), per tant aquesta situació no es pot donar. □

Definició 3.102. *Donat un graf Gf connex i simple, denotem per $\tau(Gf)$ el nombre de subgrafs de Gf que són un arbre generador.*

Exemple 3.103. *Fer exemple de $\tau(K_2)$, $\tau(K_3)$ i deixar com exercici $\tau(K_4) = 4^2$.*

Teorema 3.104. *Donat Gf connex i simple llavors $\tau(Gf) = det(MM^t)$ on $M = InDi(Gf)v_r$ on $v_r \in V(Gf)$ fixat (i aquest resultat és independent del vèrtex $v_r \in V(Gf)$ triat).*

Abans hem de recordar un resultat d'Àlgebra Lineal sobre determinants.

Teorema 3.105 (Fórmula de Binot-Cauchy)**.** *Sigui $P \in M_{N,M}(\mathbb{K})$ i $Q \in M_{M,N}(\mathbb{Q})$ amb $N \leq M$.*

Per a cada subjconjunt A_i de N elements en $\{1, \ldots, M\}$ denotem per P_i la submatriu de P de mida $N \times N$ que s'obté de triar les columnes de P $n_{i_1}, \ldots, n_{i_N}$ on $A_i = \{i_1, \ldots, i_N\}$ (i eliminar les altres columnes de P), i Q_i la submatriu de Q de mida $N \times N$ que s'obté de triar les files de Q $n_{i_1}, \ldots, n_{i_N}$ on $A_i = \{i_1, \ldots, i_N\}$ (i eliminar les altres files de Q). Llavors:

$$det(PQ) = \sum_{i=1}^{l} det(P_i) det(Q_i)$$

on $l = \begin{pmatrix} M \\ N \end{pmatrix}$.

Demostració. [fórmula] Ho fem recordant un resultat què vau demostrar alguna analogia en un seminari del curs d'àlgebra lineal (que dóno per conegut):

1. donada $X \in M_N(\mathbb{K})$, per a cada $1 \leq k \leq N$ el coeficient x^{N-k} del polinomi $det(xI_N + X)$ és la suma dels $k \times k$ menors principals de la matriu X.

2. Si $N \leq M$ amb $A \in M_{N,M}(\mathbb{K})$ i $B \in M_{M,N}(\mathbb{K})$ llavors tenim:

$$det(xI_M + BA) = x^{M-N} det(xI_N + AB) \tag{3.1}$$

Comprovem el coeficient $M-N$ en l'equació (3.1) denotant per $A = P$ i $B = Q$, del terme de la dreta és $det(AB)$ clarament.

Estudiem el coeficient $M - N$ de l'expressió de l'esquerra de (3.1). Del primer apartat tenim que és la suma de tots els menors $N \times N$ de BA, i ho podem escriure per $\sum_{S\subset\{1,\ldots,M\},|S|=N} det(BA)_{S,S}$ per la promietat multiplicativa del producte i com B té N columnes i A N files tenim que $det(BA)_{S,S} = det(B_{S,[N]})det(A_{[N],S})$ i observem si $S = A_i$ tenim $B_{S,[N]} = B_i$ i $A_{N,S} = A_i$, d'on la fórmula de Binot-Cauchy. □

Demostració. [del teorema 3.104] Denotem per $M = InDi(Gf)_{v_r}$ on $M \in M_{N-1,k}(\mathbb{Q})$, (recordem que $|V(Gf)| = N$ i treiem v_r on tenim M té $N-1$ files, ara del fet de ser Gf connex tenim $k \geq N-1$) per tant obtenim

$$det(MM^t) = \sum det(M_i)det(M_i^t) = \sum det(M_i)^2$$

sabem que $det(M_i) \in \mathbb{Z}$ i val 1 o -1 si i només si és un arbre generador, per tant obtenim el resultat. No depen de la M triada, ja que sigui quin sigui v_r obtenim el mateix resultat d'una proposició anterior. □

Exemple 3.106. *Considerem el graf* $Gf = (\{1,2,3,4,5\}, \{12,13,23,25,34,35,45\})$*, obtenim*

$$M = InDi(Gf)_5 = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ -1 & 0 & 1 & -1 & 0 & 0 & 0 \\ 0 & -1 & -1 & 0 & -1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & -1 \end{pmatrix}$$

i un càlcul obtenim $\tau(Gf) = 21$*. Deixo com exercici al lector dibuixar aquest 21 arbres generadors de* Gf*.*

Exercici 3.107 (fórmula de Cayley)**.** *Sigui* K_N *el graf simple complet d'*$N \geq 2$*-vèrtexs llavors*

$$\tau(K_N) = N^{N-2}.$$

3.5.1 Arbres amb pesos

Definició 3.108. *Una funció de cost definida en un graf connex no-trivial* $Gf = (V(Gf), E(Gf))$ *és una aplicació* $c : E(Gf) \to \mathbb{R}_{>0}$*. Si* T *és un arbre generador per a* Gf *el cost de l'arbre és* $c(T) := \sum_{e\in E(T)} c(e)$*.*

Qüestió 3.109. *Com determinar arbres generadors del graf* Gf *amb cost mínim?*

Matemàticament és clar, ja que tenim un nombre finit d'arbres generadors, i podem calcular la funció cost, i com en tenim un número finit s'agafa el mínim.

Un algoritme usual per trobar arbres de cost mínim és el següent:

Algoritme 3.110 (de Kruskal)**.** *Input/Entrada:* $Gf = (V, E)$ *graf connex* $N = |V|$.

$F_0 := \emptyset$ *% arestes arbre busquem*
for $k = 1$ *until* $N - 1$ *do:*
$F_k := F_{k-1} \cup \{b_k\}$ *on* b_k *aresta de cost minim entre les arestes* $e \in E \setminus F_{k-1}$ *on el subgraf* $H = (V, F_{k-1} \cup \{e\})$ *sigui acíclic. end for;*
Output/Sortida: $T_{Krus} := (V, F_{N-1})$.

Exemple 3.111. *Fer exemple del graf simple* $Gf = (\{1, 2, 3, 4, 5\}, \{b_1 = 12, b_2 = 23, b_3 = 34, b_4 = 35, b_5 = 24, b_6 = 25, b_7 = 15\})$ *on* $b1$ *té un cost de 1,* b_4 *un cost de 2,* b_3, b_5, b_6 *un cost de 3,* b_7 *un cost de 4 i* b_2 *un cost de 5.*

Partim aresta b_1*, primer, segon cal triar* b_4*, després podem triar una entre* b_3, b_5, b_6*, triem* b_6*, després cal triar entre* b_3 *o* b_5 *i ja finalitza on una solució és* b_1, b_4, b_6, b_3.

Transformacions elementals en un arbre

Siguin T i T' dos arbres generadors d'un graf Gf, sigui $F := E(T) \setminus E(T')$ i $F' := E(T') \setminus E(T)$. Donada $f \in F$ tenim que $T' + f$ té un cicle que anomenem Γ_f i alguna aresta de Γ_f pertany a F' (altrament T seria no aciclic).

Denotem per F_γ el conjunt d'arestes de Γ_f que pertanyen a F', alguna $f' \in F_\gamma$ es compleix que f apareix en tot cicle en $T + f'$, diem-ne un per $\Gamma_{f'}$ de $T + f'$ (en cas contrari $\Gamma_f \cup \Gamma_{f'}$ té un cicle sol per arestes de T, cosa no factible), per tant obtenim que

$$T_1 = (T + f') - f$$

és un arbre generador per a Gf on número arestes en T' és una més i el nombre comú arestes en T és una menys, e iterant aquest procediment arribem de l'arbre generador T a l'arbre generador T', en particular T_1 s'anomena una **transformació elemental de l'arbre generador** T **de** Gf, i obtenim en particular:

Lema 3.112. *Donats* T, T' *dos arbres fonamentals d'un graf connex* Gf*, via transformacions elementals podem anar de l'arbre* T *a l'arbre* T'.

Lema 3.113. *Sigui* T *un arbre generador d'un graf connex* Gf *de cost mínim* $\Leftrightarrow$ $c(T') \geq c(T)$ *for all* $T' \in \mathcal{C}(T)$ *on* $\mathcal{C}(T)$ *corresponen a tots els arbres generadors de* Gf *que s'obtenen aplicant UNA transformació elemental al graf* T.

Demostració. $\Rightarrow$ és evident. $\Leftarrow$: Sigui T un arbre on $c(T') \geq c(T)$ on $T' = T + f' - e$ arbre generador, i sigui T_m un arbre generador de Gf de cost mínim. Denotem per $F := E(T) \setminus E(T_m)$ i $F_m := E(T_m) \setminus E(T)$.

Donat $f \in F$, sigui $h \in F_m$ aresta del cicle $\Gamma_f = T_m + f$ i considerem l'arbre generador

$$T' = (T + h) - f$$

Com $T' \in \mathcal{C}(T)$ tenim que $c(T') \geq c(T)$ i per tant $c(h) \geq c(f)$.

Ara considera l'arbre generador $T'_m = (T_m + f) - h \in \mathcal{C}(T_m)$ per minimalitat tenim $c(T'_m) \geq c(T_m)$ d'on $c(f) \geq c(h)$ i per tant $c(f) = c(h)$.

Per iterar el procediment ens falta demostrar que $c(T'') \geq c(T')\ \forall T'' \in \mathcal{C}(T')$, un cop demostrat tenim fent transformacions elementals arribem de T a l'arbre T_m amb arbres de cost $c = c(T_m)$ i per tant T és un arbre generador de cost mínim per a Gf.

Demostrem doncs:$c(T'') \geq c(T')\ \forall T'' \in \mathcal{C}(T')$. Suposem el contrari on $T'' = (T' + h') - f' \in \mathcal{C}(T')$ on $c(T'') < c(T')$ on $h' \notin E(T')$ i $f' \in E(T')$.

Tenim $T' + h'$: (i) té un cicle $\Gamma_{h'}$ que no conté h com $T' = T + h - f$ tenim $\Gamma_{h'}$ es un cicle de $T + h'$ i $(T + h') - f' \in \mathcal{C}(T)$ on tindria un cost menor que T cosa que no pot ser per el.lecció de T, (ii) tot cicle $\Gamma h'$ conté h, i considerem $\Gamma_{h'} \cup \Gamma_h$ on Γ_h cicle de $T + h$, obtenim que conté un unic cicle $\Gamma^{'}_{h'}$ de $T + h'$ i $f' \in \Gamma^{'}_{h'}$ per tant $(T + h') - f'$ té cost menor que T cosa tampoc possible. Per tant aquesta situació no es pot donar. □

Demostració. [algorisme de Kruskal] Tenim que T_{Krus} té $N - 1$ arestes i aciclic per construcció i té exactament N vèrtexs.

Suposem que tingui k components connexes $T_1, \ldots, T_k$, on T_i són arbres i per tant

$$N - 1 = |E(T_{Krus})| = \sum_{i=1}^{k} (|V(T_i)| - 1) = N - k$$

per tant $k = 1$ i per tant és connex.

Si existís $T' = (T_{Krus} + h) - f \in \mathcal{C}(T_{Krus})$ amb $c(T') < c(T_{Krus})$ per la demostració del lema anterior tenim que $c(h) < c(f)$ però per FOR THEN de l'algoritme no pot ser haver fet aquesta tria, per tant pel lema anterior obtenim que T_{Krus} és un arbre generador de cost mínim. □

3.6 Grafs planars

Definició 3.114. *Un graf Gf amb $N = |V(Gf)|$ i $M = |E(Gf)|$ diem que és planari si pot ser dibuixat en el plà $\mathbb{R}^2$ sense talls amb les arestes. Parlem de graf plà si aquest dibuix és fixat.*

En el curs de topologia fixareu aquest resultat que queda fora d'aquest curs:

Teorema 3.115 (de la corba de Jordan)**.** *Un cicle d'un graf plà divideix el pla en dues regions, interior i exterior.*

No hi pot haver cap aresta entre un vèrtex interior i un vèrtex exterior a un cicle. [3]

Un graf pla Gf divideix el pla en un cert nombre de regions, on una regió és una porció maximal del pla verificant que qualsevol parell de punts d'aquesta regió es poden unir-se mitjançant una (secció d'una) corba plana C tal que cap punt d'ella interseca a les corbes entre les arestes del graf pla.

Teorema 3.116 (fórmula d'Euler)**.** *Si R és el nombre de regions d'un graf pla Gf connex amb $N = |V(Gf)|$ i $M = |E(Gf)|$, llavors*

$$N - M + R = 2$$

Exemple 3.117. *Dibuixar un graf plà (i comentar la diferència en graf planari). Per exemple fem K_4 es graf planari, però el dibuix usual no és un graf pla, però altres sí, veieu apunts de classe teoria.*

[3] Aquest resultat també s'enuncia com: tota corba tancada (simple) en $\mathbb{R}^2$ divideix el pla en dos components regions disjuntes que tenen la corba tancada com frontera entre aquestes dues regions. La regió acotada s'anomena interior, la no acotada s'anomena exterior.

Demostració. Fem inducció respecte M. Per a $M = 0$ tenim que $N = 1$ per a ser connex i $R = 1$.

Considerem ara un Gf graf pla connex amb $|E(Gf)| = M+1$ on $N = |V(Gf)$ i R número de regions del graf. Si no té cap cicle, llavors és un arbre i per tant $|V(Gf)| = M + 2$ i $R = 1$ d'on es compleix la fórmula d'Euler. En cas que tingui un cicle, sigui $a$una aresta d'aquest cicle, considerem el graf pla $Gf \setminus a$ (de treure el dibuix de l'aresta a), continua sent connex i ara $|E(Gf \setminus a)| = M$ i el nombre de regions es una menys que Gf, per hipòtesi d'inducció en el graf $Gf \setminus a$ obtenim:

$$|V(Gf \setminus a)| - |E(Gf \setminus a)| + (R - 1) = 2$$

i per tant $N - (M) + (R - 1) = 2$ d'on $N - (M + 1) + R = 2$ per tant obtenim la fórmula d'Euler pel graf Gf. □

Observació 3.118. *Anem en aquesta observació intentem aportar una altra demostració de la fórmula d'Euler usant graf dual d'un graf pla.*

Definició 3.119. *Sigui Gf un graf simple (o multigraf o pseudograf) pla, assignarem un graf Gf^* de la manera següent: per a cada regió posem en l'interior un vèrtex anomen c^* i aquests corresponen als vèrtexs per $V(Gf^*)$, per a cada aresta $e \in E(Gf)$ entre dues regions r_1, r_2 on hem assignat vèrtexs de Gf^* c_1^* i c_2^* respectivament assignem $e^* \in E(Gf^*)$ on e^* aresta entre c_1^* i c_2^*, i d'aquesta manera construïm totes les arestes de Gf^*. En particular $|E(Gf)| = |E(Gf^*)|$.*

Sigui T un arbre generador en un graf Gf pla. Anem a definir un subgraf T^* de Gf^* de la forma següent on $V(Gf^*) = V(T^*)$. El conjunt $E(T^*) \subset E(Gf^*)$ estarà amb bijecció amb $E(Gf) \setminus E(T)$ i s'obté de la manera següent: una aresta de $E(Gf) \setminus E(T)$ conecta una regió amb una altra regió ja que conté un cicle i triem una aresta e^* que conecta aquestes dos cares per aquesta aresta per $e^* \in E(T^*)$, i ho fem en totes les situacions. Observem com es pla, d'una cara podrem anar a una altra via arestes de $E(T^*)$ i per tant T^* és un graf connex. Deixem com exercici al lector demostrar que T^* és acíclic.

Per tant T^* és un arbre generador per a Gf^*.

Demostrem ara la fórmula d'Euler amb la noció de graf dual introduïda en aquesta observació:

Demostració. [fórmula Euler usant graf dual] Considerem Gf graf pla, i T un arbre generador, anotem $e_T = |E(T)|$ i $N = |V(Gf)| = |V(T)|$ i sabem que $N = e_T + 1$. Considerem Gf^* i T^* arbre generador de Gf^* construït anteriorment, i denotem $e_{T^*} = |E(T^*)|$ i sabem que $R = |V(Gf^*)|$ el nombre de regions del graf pla Gf, i per ser arbre $R = e_{T^*} + 1$. Per construcció de T^* tenim $e_T + e_{T^*} = |E(Gf)|$. Per tant obtenim:

$$N + R = e_T + 1 + e_{T^*} + 1 = |E(Gf)| + 2$$

obtenint la fórmula d'Euler. □

Recordem que si Gf és un graf simple (o multigraf o pseudograf) i denotem per $N = |V(Gf)|$, i N_i el $\# \, v \in V(Gf)$ amb $deg(v) = i$ tenim que

$$N = N_0 + N_1 + \dots$$

pel lema d'encaixada de mans (demostreu el lema d'encaixada de mans 3.15 pel cas de multigraf o pseudograf) obtenim:

$$2e := 2|E(Gf)| = \sum_{i=1}^{\infty} i \cdot N_i = N_1 + 2N_2 + 3N_3 + \dots$$

Anomenem el grau mitjà del graf Gf al valor $\overline{d}(Gf) := \frac{2e}{N}$.

Suposem que Gf és un graf pla, i una k-regió del graf pla denota una regió envoltada exactament per k-arestes, i denotem per f_k el nombre de k-regions del graf Gf.

Observació important: si una aresta no està en CAP cicle de Gf, la regió que envolta l'aresta la comptem que envolta l'aresta per les dues cares, per exemple si sol tenim una aresta uv i el graf es $(\{u, v\}, \{uv\})$, sol té una regió però la pensem aquesta regió com que és una 2-regió, si tenim que Gf és un arbre T que es pla amb k arestes té l'arbre, sol tenim una regió però aquesta regió la pensem com una $2k$-regió ja que recorrem pels dos costats cada aresta de l'arbre

Si denotem per R el total de regions del graf Gf tenim llavors:

$$R = \sum_{i=1}^{\infty} f_i = f_1 + f_2 + \dots$$

Lema 3.120. *Amb la notació anteriorment tenim la igualtat:*

$$2e = f_1 + 2f_2 + 3f_3 + \ldots = \sum_{i=1}^{\infty} i \cdot f_i$$

i definit el nombre de cares (faces) mitjà del graf pel valor $\overline{fac} := \frac{2e}{R}$.

Demostració. Considerem la suma: $M := f_1 + 2f_2 + 3f_3 + \ldots = \sum_{i=1}^{\infty} i \cdot f_i$. Observem que cada aresta del graf que es trobi en un cicle del graf apareix exactament en dues regions i per tant es compta 2 en el sumands de M. Ara, cada aresta del graf que no es troba en cap cicle es troba dins una k-regió on dins el k compta les dues cares de l'aresta i per tant en fer kf_k, cada k-regió si assignem k arestes, en particular cada aresta que no està en cap cicle suma 2 en el sumatori per a cada una d'aquestes arestes que no es troba en cap cicle. Per tant exactament cada aresta contribueix 2 cops en M on $2e \leq M$. Fixem-nos que kf_k compta per cada k-regió 1 cop les arestes que es troben en un cicle (que es tornaran a comptar en una altra regió) i 2 cops per les arestes en la k-regió que no es troben en cap més regió i per tant tenim $M \leq 2e$. □

Lema 3.121. *El graf complet K_5 no és un graf planar.*

Demostració. Tenim $N = |V(K_5)| = 5$ i $e = |E(K_5)| = \begin{pmatrix} 5 \\ 2 \end{pmatrix} = 10$ on tenim si fos planar que $R = e+2-N = 7$ per la fórmula d'Euler, i per tant $\overline{fac} = \frac{20}{7} < 3$. Per tant hi ha una cara amb com a molt 2 arestes (ja que si totes tenen 3 arestes o més tenim $2e = 3f_3+4f_4+\ldots \geq 3(f_3+f_4+\ldots)$ i $R = f_3+f_4+\ldots$ i tenim que $\overline{fac} \geq \frac{3(R)}{R} \geq 3$). Per tant surt que ha de tenir un cara amb dos arestes, per tant el graf pla ha de ser un multigraf (dos arestes anant entre dos vèrtexs diferents) però K_5 no és cap multigraf, sino un graf simple, per tant no és possible. □

Definició 3.122. *Un graf simple Gf s'anomena bipartit si el conjunt $V(Gf) = V_1 \cup V_2$ amb $V_1 \cap V_2 = \emptyset$ i compleix que $\forall e \in E(Gf)$ els vertexs incidents amb e és un vèrtex de V_1 i un vèrtex de V_2. Si a més cada vèrtex de V_1 és adjacent a tots els vèrtexs de V_2, diem que el graf bipartit Gf és complet.*

Exemple 3.123. *Considera el graf $Gf = (\{1,2,3,4,5\}, \{14,15,24,25,34,35\})$ és bipartit $V_1 = \{1,2,3\}$ i $V_2 = \{4,5\}$ i a més complet. Correspon al $K_{3,2}$.*

Lema 3.124. *Els grafs bipartits complets Gf on $|V_1| = N$ i $|V_2| = M$ amb $|V(Gf) = V_1 \cup V_2| = N + M$ son tots isomorfs (exercici al lector) i s'anota aquest graf bipartit per $K_{N,M}$.*

Lema 3.125. *El graf $K_{3,3}$ no és un graf planar.*

Demostració. Observem que $|V(K_{3,3})| = 6$ i $|E(K_{3,3})| = 9$ i per tant si fos planar per la fórmula d'Euler obtenim que $R = e + 2 - N = 5$ i per tant $\overline{fac} = \frac{18}{5} < 4$.

Ara el graf $K_{3,3}$ cada cicle té longitud ≥ 4, i per tant cada regió és almenys una 4-regió, i per tant $\overline{fac} \geq 4$ si fos planar, cosa impossible. □

Enunciem un teorema fora del contingut del curs, tant sols per saber que es poden caracteritzar els grafs planars.

Teorema 3.126 (Kuratowski, (Frink-Smith), 1930)**.** *Sigui Gf un graf connex (multigraf o pseudograf) planar si i només si no hi ha cap subgraf "homeomorf" a $K_{3,3}$ o a K_5.*

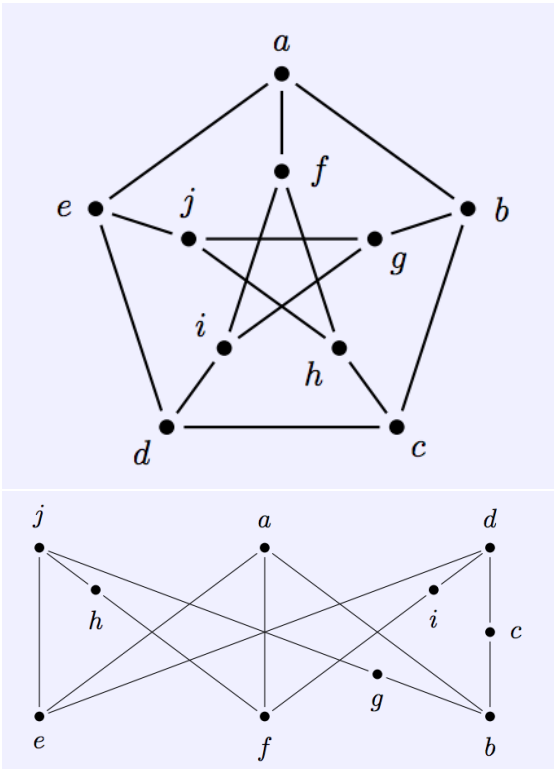
Observació 3.127. *Anem a detallar el concepte subgraf "homeomorf" en aquesta observació. Detallarem tres conceptes:*

- *Una subdivisió elemental d'un graf Gf consisteix a eliminar una aresta uv del Gf i afegir-hi un nou vèrtex w i dues arestes uw i wv. (podem pensar en una aresta d'un graf afegir-hi al mig un vèrtex de grau 2). Aquesta operació no afecta la planaritat del graf.*

- *Una subdivisió d'un graf Gf és un graf que s'obté a partir de Gf mijançant una successió de subdivisions elementals, en particular continua mantenint la planaritat.*

- *Dos grafs Gf_1 i Gf_2 diem que són homeomorfs si existeix un graf Gf tal que Gf_1 sigui isomorf a Gf o a una subdivisió de Gf i el graf Gf_2 sigui isomorf a Gf o a una subdivisió de Gf.*

Exemple 3.128. *El graf de Petersen té un subgraf que és homeomorf a $K_{3,3}$, veieu les imatges següents:*



Observació 3.129. *Hi ha un resultat anàlog al de Kuratowski però usant la noció contràctil enlloc de homeomorf. Anem a donar-ne els mínims aquí. En el curs de topologia veure la noció contràctil com homeomorf que serà conceptes esencials.*

Diem que fem una contracció elemental en un graf quan en una aresta uv del graf la contraiem, és a dir substituim l'aresta i els vèrtexs u, v tot per un únic vèrtex e (mantenint tot l'altre del graf en particular les altres arestes del graf que tenien per veïns els vèrtexs u ó v, els mantenim però després de la contracció elemental tenen com vèrtex adjacent w enlloc de v o u).

Una contracció en un graf Gf consisteix en aplicar una successió de contraccions elementals en el graf, observeu que manté la planaritat.

Diem que dos grafs Gf_1 i Gf_2 són contraïbles un a l'altre, si existeix un graf Gf on una contracció arribem al graf Gf_1 i amb una altra contracció obtenim el graf Gf_2.

Teorema 3.130 (Harary-Tutte, Wagner)**.** *Tot graf Gf és planari si i només si cap subgraf és constraïble a K_5 ó a $K_{3,3}$.*

Proposició 3.131. *Sigui Gf un graf simple plà connex no buit ambà almenys dos arestes. Llavors:*

- *Gf té almenys un vèrtex de grau com a molt 5.*
- $|E(Gf)| \leq 3|V(Gf)| - 6$.

Demostració. Comencem pel primer item: sabem que cada cara té almenys 3 arestes (ja que Gf és un graf simple) i per tant $R = f_3 + f_4 + \ldots$ i $2e =$

$3f_3 + 4f_4 + \ldots$ per tant

$$2e - 3R \geq 0$$

Ara si cada vèrtex té grau ≥ 6 tenim $N = |V(Gf)| = N_6 + N_7 + \ldots$ i $2e = 6N_6 + 7N_7 + \ldots$ per tant

$$2e - 6N \geq 0$$

i per tant

$$6(e - N - R) = (2e - 6N) + 2(2e - 3R) \geq 0$$

d'on obtenim $e \geq N + R$ però ara per la fórmula d'Euler $N - e + R = 2$ en contradicció.

Pel segon item: amb argument similar com anterior item obtenim que $2e - 3R \geq 0$ d'aquí observem

$$3N - 6 = 3(2 + e - R) - 6 = 3e - 3R \geq e = |E(Gf)|$$

on en la primera igualtat hem usat la fórmula d'Euler. □

3.6.1 Pintant grafs planars

Qüestió 3.132. *Si tenim un graf plà connex i volem pintar els vèrtexs de colors on vèrtexs adjacents tenen colors diferents (no pintem les arestes). Quin és el nombre minim de colors per poder-ho fer? Diem que un graf és k-colorable si amb k colors diferents podem pintar els vèrtexs del graf on vèrtexs adjacents tenen colors diferents.*

Definició 3.133. *Sigui Gf un graf simple i connex. Diem que Gf és k-colorable si amb k colors diferents podem pintar els vèrtexs del graf on vèrtexs adjacents tenen colors diferents. Definim el nombre cromàtic d'un graf Gf simple i connex com el natural $\chi(Gf)$ on el Graf Gf és $\chi(Gf)$-colorable però no és $\chi(Gf) - 1$-colorable.*

Lema 3.134. *Tot graf connex planar és 6-colorable.*

Demostració. Sigui Gf un graf planar connex, i $N = |V(Gf)|$. Per a $N \leq 6$ és obvi que és 6-colorable. Argumentem-ho per inducció respecte $N = |V(Gf)|$, on de ser connex i $N \geq 6$ té almenys 3 arestes.

Per la proposició 3.131 tenim que $\exists v \in V(Gf)$ amb $deg(v) \leq 5$, per tant v té com a molt 5 veïns. Considera $Gf' := (V(Gf)\backslash\{v\}, E(Gf)\backslash\{arestes\ adjacents\ amb\ v\})$ (treiem el vèrtex i les com a molt 5 arestes que contenien aquest vèrtex). El graf Gf' continua sent un graf planari amb $N - 1$ vèrtex, per tant 6-colorable per inducció si Gf' és connex. Si Gf' no és connex cada component connexa serà un graf plà i connex i per tant 6-colorable. Ara cal estendre la 6-coloració de Gf' a Gf.

Ara dels com a molt 5 veïns de v tenen assignats com a molt 5 colors diferents, per tant podem estendre la coloració en el vèrtex v amb un color diferent dels seus veïns, i per tant tenim que Gf és 6-colorable. □

Definició 3.135. *Donar un graf Gf simple i conex. El* nombre cromàtic de llistes *de Gf, denotat per $\chi_\ell(G)$, és el mínim enter k tal que, per a* tota *assignació de llistes*

$$L(v) \subseteq \mathbb{N}, \qquad |L(v)| = k \text{ per a tot } v \in V,$$

existeix una coloració pròpia c que satisfà

$$c(v) \in L(v) \quad \textit{per a tot } v \in V.$$

Cada vèrtex pot tenir, doncs, el seu propi conjunt de colors permesos.

Lema 3.136. *Per a qualsevol graf Gf connex i simple tenim $\chi(G) \leq \chi_\ell(G)$.*

Demostració. En efecte, si prenem $L(v) = \{1, \ldots, k\}$ per a tot $v \in V(Gf)$, una coloració de llistes és simplement una k-coloració usual. □

Observació 3.137. *Recordem que un* mapa pla *és una partició del pla en regions connexes, anomenades països, de manera que dues regions es consideren adjacents si comparteixen un segment de frontera (no només un punt). A partir d'un mapa plà es pot definir un graf Gf de la manera següent:*

1. *els vèrtexs de Gf corresponen a les regions del mapa;*
2. *hi ha una aresta entre dos vèrtexs si les regions corresponents són adjacents.*

Fixeu-nos que el graf Gf és simple, és connex i és planar. El teorema dels 4-colors afirma que aquest graf compleix $\chi(Gf) \leq 4$.

La demostració que tot graf simple i connex Gf compleix que $\chi(Gf) \leq 4$ i per tant 4-colorable és fora de l'abast del curs, nosaltres provarem que $\chi(Gf) \leq 5$, realment demostrarem que $\chi_\ell(Gf) \leq 5$ en aquest curs.

Una conjectura de Erdös-Rubin-Taylor afirmava que tot graf simple connex i planar compleix $\chi_\ell(Gf) \leq 5$ i que existeixen Gf grafs simples, connex i planars amb $\chi_\ell(Gf) = 5$.

Margit Voigt l'any 1993 in [Vo93] construeix un graf planar simple connex amb $\chi_\ell(Gf) = 5$.

Teorema 3.138. *Tots els grafs simples connexos i planars Gf són 5-colorables i per tant $\chi(Gf) \leq 5$.*

Observem primer: si denotem per $k = col(Gf)$ el natural mínim on el graf Gf és k-colorable, i si Hf és un subgraf de Gf tenim que

$$col(Hf) \leq col(Gf)$$

i per tant en un graf planar i podem anar afegint arestes (dins regio) de manera que no s'intesequin, i cal veure que aquest grafs amb més arestes compleixen que són 5-colorable.

Abans d'iniciar la demostració del resultat, assumim que si tenim una regió tancada amb $k \geq 3$ arestes, llavors afegint arestes entre vèrtexs no adjacents podem subdividir aquesta regió amb regions que formen triangles (és dir regions amb exactament 3 arestes) i si el problema de coloració funciona per aquests grafs amb triangles tenim el cas general. (En el llenguatge de topologia és fer una triangularització de la regió)

Demostració. Considerem doncs un graf planar on suposem que les cares (regió) acotades del graf estan formades per triangles.

Denotem per Out el cicle que recorre la regió exterior del graf pla escrivim $Out = u_1u_2 \ldots u_tu_1$ on $u_i \in V(Gf)$.
Sigui l'enunciat següent:

- Els vertexs u_1 i u_2 estan pintats amb el color 1 i el color 2 respectivament.
- Cada vèrtexs de Out llevat del u_1 i u_2 tenen una llista d'almenys TRES colors que podem elegir per a pintar-lo.
- Cada vèrtexs del Gf llevat dels que surten en el cicle Out, tenen una llista d'almenys CINC colors que podem elegir per a pintar-lo.

I la conclusió de l'enunciat és que podem estendre la coloració inicial de u_1 i u_2 a tot el graf Gf.

Demostrem aquest enunciat per inducció respecte $N = |V(Gf)|$ amb $N \geq 3$.

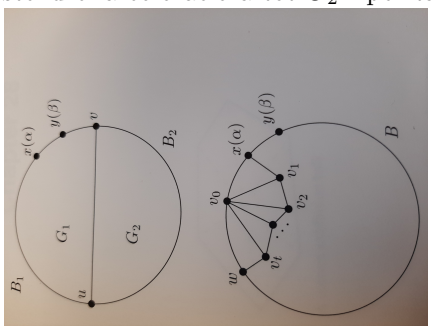
El cas $N = 3$, tenim un triangle i cicle $u_1u_2u_3u_1$ on u_1 i u_2 estan pintats, com en el vèrtex u_3 tenim una llista de 3 colors un d'ells serà diferent al color 1 i al color 2, per tant podem estendre la coloració al vèrtex u_3 triant un color de la llista dels 3 que hi ha (i no sigui color 1 ni color 2).

Suposem cert el cas per tots grafs planars connexos simples amb número de vèrtexs $\leq N - 1$ i cal veure per grafs amb número de vèrtexs N.

Escrivim $Out : u_1u_2 \dots u_tu_1$.

- Cas I: Hi ha dos vèrtexs diferents u_i, u_j diem-los-hi u i v que es troben en Out on hi ha una aresta en Gf que els uneix i no es troba en Out.

  Podem considerar dos subgrafs de Gf planars connexos i simples: graf G_1 on el circuit que el tanca és $B_1 \cup \{uv\}$ i que conté u_1 i u_2 (que anomenem x (amb color 1 anomenat α) e y (amb color 2 anomenat β) respectivament). Observem que B_1 continua esent triangular i té menys que N vèrtexs, per hipòtesi d'inducció tenim el resultat. Anomenem ara el color associat en aquesta coloració al vèrtex u per γ i al vertex v per δ i mirem ara el graf pla connex G_2 que de nou té menys d'N-vèrtexs i per tant aplicant la inducció podem estendre la coloració a tot G_2 i per tant obtenim que la coloració s'estén.



- Cas II: No hi ha cap aresta unint vèrtexs de Out que no es trobi en el cicle Out. Diem x a u_1 amb el color 1 (anomenem α) i anomenem y a u_2 amb el color 2 (que anomenem β), si sigui v_0 el vèrtex a l'altre costat de x en el cicle Out. Considerem tots els veïns del vèrtex v_0 del graf Gf que son dins Out els vèrtexs: x i w i a dins del graf corresponen a $v_1, \dots, v_t$, i formant $v_0v_iv_{i+1}v_0$ una regió-triangle del graf Gf (veieu la figura anterior).

  Considerem el graf $Gf' := (V(Gf)\backslash\{v_0\}, E(Gf)\backslash\{wv_0, v_0x, v_0v_1, \dots, v_0v_t\})$ i fixeu-vos que continua sent Gf' planar graf simple i connex amb menys vèrtexs que Gf. El cicle exterior per a Gf', que anomenem Out' consisteix en treure v_0 i les arestes wv_0 i v_0x i afegir els vèrtexs: $v_1, \dots, v_r$ i

les arestes: $wv_t, v_tv_{t-1}, \ldots, v_2v_1, v_1x$. Ara com el vèrtex v_0 podia elegir tres colors i x està pintat pel color α tenim que hi ha dos colors γ, δ que podem triar pel vèrtex v_0 (compatible amb el color triat per a x). Ara de la llista de colors que tenien tots els v_i's que eren 5, treiem de la llista els colors γ, δ i per tant es queden amb una llista d'almenys 3 colors diferents aquest vèrtexs. Llavors Gf' amb el color α triat per a x i β triat per a y tenim distribuit totes les condicions de l'enunciat per a concloure que podem estendre la coloració a tot Gf'. Ara sol falta triar la coloració pel vèrtex v_0 pero per aixo ho triem diferent del color que té el vèrtex w i el color α que té el vèrtex x i és factible ja que té tres colors per a triar i tots els altres veins s'han colorejat amb una llista de colors que no té γ i δ. I per tant podem estendre la coloració a tot el graf.

□

Observació 3.139. *Realment demostrem en l'anterior prova que donat Gf simple, connex i planar llavors $\chi_\ell(Gf) \leq 5$ i en particular $\chi(Gf) \leq 5$.*

3.7 Algunes aplicacions de grafs amb àlgebra lineal

3.7.1 Amics i polítics

En un grup de persones tenim la situació que qualsevol parella de dues persones tenen exactament un amic en comú. Aleshores sempre hi ha una persona (el "polític") que és amic de tots. Parlarem del teorema de l'amistat.

Reformulem primer el problema usant la teoria de grafs.

Interpretem les persones com el conjunt de vèrtexs $V(Gf)$ d'un graf Gf i unim dos vèrtexs per una aresta de Gf si i només si les persones corresponents són amics, pensant que l'amistat és sempre bidireccional, és a dir, si u és amic de v, llavors v també ho és de u i, a més, ningú és el amic d'ell mateix. Així observem que Gf és un graf simple.

Teorema 3.140 (Teorema de l'amistat, II)**.** *Suposem que Gf és un graf simple on dos vèrtexs $v_1, v_2 \in V(Gf)$ amb $v_1 \neq v_2$ tenen exactament un veí comú. Llavors existeix un vèrtex que és adjacent a tots els altres vèrtexs del graf Gf.*

Observació 3.141. *Un altre enunciat que també és coneix com teorema de l'amistat correspon al següent enunciat: en qualsevol grup de 6 o més persones sempre hi ha o bé un grup de 3 persones que es coneixen mútuament o bé un grup de 3 persones que no es coneixen. Recordeu que aquest enunciat correspon a l'existència de triangles o anti-triangles al principi del tema de grafs.*

Lema 3.142. *Considerem Gf en les hipòtesis del teorema de l'amistat. Suposem que existeix dos vèrtexs $u, v \in V(Gf)$ no adjacents on $deg(u) \geq 3$. Llavors Gf és un graf regular, és a dir $d(v) = k\ \forall v \in V(Gf)$ i es té $|V(Gf)| = k^2 - k + 1$.*

Demostració. Observem primer que el graf Gf no te cicles de longitud 4, ja que llavors dos vertexs tenen almenys 2 veïns comuns.

Provem primer que si $u, v \in V(Gf)$ no adjacents llavors $deg(u) = deg(v)$. Siguin $u_1, \ldots, u_k$ els veïns de u, i per hipòtesis, exactament un d'ells és adjacent

a v, diem-li u_2. Aquest u_2 és adjacent exactament a un dels $u_i's$ $i \neq 1$ (u_2, u exactament 1 amic en comú), denotem-lo per u_1.

El vèrtex v amb u_i per a $i \geq 2$ té exament un veí comú, anomenem-los z_i per $i \geq 2$. Aquests z_i's s'on diferents, altrament $uu_iz_iu_ju$ formaria un 4-cicle si $z_i = z_j$, per tant $z_i \neq z_j$ i obtenim que $deg(v) \geq k = deg(u)$. Intercanviant els papers de u i v obtenim l'altra desigualtat.

Per tant $deg(u) = deg(v)$ si $u, v \in V(Gf)$ no adjacents.

Ara, fixem-nos que tot vèrtex que no és u_2 o bé no és adjacent a u o bé no és adjacent a v, i per tant té grau k. Ara si u_2 no és adjacent a algun vèrtex del graf Gf, també tindrà grau k, observem que no pot ser adjacent a tot vèrtex del graf perquè com $k \geq 3$, algun dels z_i's amb $i \geq 3$ és no adjacent a u_2 ja que si ho for tenim un cile de longitud 4: uz_2vz_3u. Per tant tot vèrtex del Gf compleix $deg(v) = k$.

Sumant sobre els graus dels k veins de u obtenim k^2. Ara com cada vèrtex de Gf (llevat de u) té exactament un veí amb u, hem comptat cada vèrtex un cop llevat del vèrtex u que s'ha comptat k vegades, i per tant

$$|V(Gf)| = k^2 - k + 1.$$

□

Observació 3.143. *Reseguint la demostració del lemma anterior, observem que si tenim un $u, v \in V(Gf)$ no adjacents amb $deg(u) = 2$, llavors $deg(v) = 2$ i obtenim $deg(u_2) \geq 4$. Si hi ha un tercer vertèx $v_2 \in V(Gf)$ no adjacent obtenim un $deg(u_2')\deg 4$ però u_2' ha de ser adjacent a u i v altrament tindria grau 2 i per tant ha de ser u_2. Iterant, obtenim els anomenats grafs moliNs de vent.*

En el cas que tot vertex $u, v \in V(Gf)$ no adjacent té $deg(u) = 1$, sortiria una estrella (arbre amb un vèrtex al mig i els raigs representen les diferents arestes) però llavors entre aquest vèrtex central i un altre, no hi ha un únic amic comú i per tant no es pot donar aquest cas.

Lema 3.144. *No existeix cap graf Gf simple regular amb $deg(v) = k \geq 3$ per a tot $v \in V(Gf)$ complint $|V(Gf)| = k^2 - k + 1$ i que donat dos vèrtexs no adjacents hi hagi exactament un vèrtex veí d'ambdos.*

Demostració. Considerem la matriu adjacent del graf simple Gf: $Ad(Gf)$. Cada columna de $Ad(Gf)$ té k posicions 1's i $k^2 - 2k + 1$ posicions de zeros. A més del fet que "donat dos vèrtexs no adjacents hi hagi exactament un vèrtex veí d'ambdos" tenim

$$Ad(Gf)^2 = \begin{pmatrix} k & 1 & \dots & 1 \\ 1 & k & & 1 \\ \vdots & & \ddots & \\ 1 & \dots & 1 & k \end{pmatrix} = (k-1)I_{k^2-k+1} + \mathbb{1}_{k^2-k+1}$$

on $\mathbb{1}_n$ és la matriu $n \times n$ on totes les entrades són igual a 1, on la igualtat per a $Ad(Gf)^2$ prové del Proposició 3.35 i de les condicions del nostre graf.

Tant $Adj(A)^2$, I_n i $\mathbb{1}_n$ són simetriques i per tant diagonalitzables. És fàcil demostrar que $\mathbb{1}_n$ té el valor propis n (de multiplicitat 1) (un vector propi és $(1, \dots, 1)$) i el valor 0 (de multiplicitat $n-1$) i per tant (exercici al lector) $Ad(Gf)^2$ te valors propis $k - 1 + (k^2 - k + 1) = k^2$ (de multiplicitat 1) i $k - 1$ (de multiplicitat $k^2 - k$).

També $Ad(Gf)$ simètrica per tant diagonalitzable, i fàcilment que té valor propi k (de multiplicitat 1) i $\pm\sqrt{k-1}$. Suposem que $r_1 = dim(Ker(Ad(Gf) - \sqrt{k-1}I_{k^2-k+1}))$ i $r_2 = dim(Ker(Ad(Gf)+\sqrt{k-1}I_{k^2-k+1}))$ on $r_1+r_2 = n-1 = k^2-k$.

Com la suma dels valors propis de matriu diagonal (amb multiplicitat) és igual a la traça de $Adj(Gf)$ que és zero (graf simple) obtenim

$$k + r_1\sqrt{k-1} - r_2\sqrt{k-1} = 0,$$

en particular $r_1 \neq r_2$ ja que $k \neq 0$, obtenint que $\sqrt{k-1} = \frac{k}{r_2-r_1}$ on $\sqrt{k-1}$ és un enter, diem-lo int (exercici al lector) i obtenim

$$int(r_2 - r_1) = k = int^2 + 1$$

per tant int divideix $int^2 + 1$ i també divideix int^2, per tant $int = 1$ i obtenim que $k = 2$, però sempre $k \geq 3$ estem suposant, per tant no es possible aquesta matriu $Ad(Gj)$ □

Demostració. [Teorema 3.140] Pel lemma 3.142 i l'observació de després s'obté un graf on $Ad(Gf)^2$ és com indicada en la demostració del Lemma 3.144 i per tant no és possible si algun vèrtexs amb vèrtexs no adjacents té grau ≥ 2. Gràcies a la demostració del Lemma 3.142 i l'observació que el segueix, si té dos vèrtexs adjacents té grau 1 o 2, llavors tots els no adjacents tenen mateix grau i llavors per tal que compleixi el teorema correspon al que s'anomenen grafs de molins de vent, i que per tant sempre tenen un vèrtex adjacent a tots els altres vèrtexs. □

3.7.2 Algorisme del PageRank

El PageRank de Google $PR(X)$ és un número que s'assigna a cada plana X per a mesurar la seva importància. Aquest número s'utilitza per a ordenar les cerques, de manera que surten en primer lloc les que tenen el PageRank més elevat.

Transllademem el problema a un graf dirigit, on cada pàgina correspon a un vèrtex del graf, i un enllaç de la pàgina A a la pàgina B és una aresta dirigida AB.

Exemple 3.145. *Considerem 4 pàgines web: A, B, C i D de manera que tenim un enllacc DC, BC, AC, AB i CA i per tant obtenim un graf dirigit amb vèrtexs $\{A, B, C, D\}$ i arestes dirigides $\{DC, BC, AC, AB, CA\}$.*

Tenim doncs:

- *La pàgina A té dos enllaços: $n_A = 2$ (i la plana C l'enllaça)*
- *La pàgina B té un enllaç: $n_B = 1$ (i la plana A l'enllaça)*
- *La plana C té un enllaç: $n_C = 1$ (i l'enllacen les webs: A, B i C)*
- *La plana D té un enllaç: $n_D = 1$ i no l'enllaça cap plana.*

Fixem un nombre mínim d'importància (les webs no tenen cap enllaç): $0 < p \leq 1/2$.

Iniciem el procediment fent que $PR(X) = 1$ per a una col.lecció finita pàgines web $X_1, \ldots, X_n$, diem el vector d'inici $PR_0 = \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} \in M_{n,1}(\mathbb{R})$, considerem n_{X_i} el nombre d'enllaços de la pàgina X_i a una altra web de la llista $X_1, \ldots, X_n$ i definim la matriu $M \in M_{n,n}(\mathbb{R})$ on

$$(M)_{i,j} := \frac{\delta_{i,j}}{n_{X_j}}$$

on $\delta_{i,j}$ és 1 si hi ha un enllaç de la web X_i a la web X_j i 0 altrament. Fixeu-vos que la suma dels coeficients de cada columna dóna sempre 1 (i tots els valors són ≥ 0)

Definim una recurrència via

$$PR_k := (1-p)MPR_{k-1} + pPR_0$$

i es prova tots els coeficients de PR_k són positius, i la suma de tots els coeficients de PR_k és n.

Fàcilment podem escriure aquesta recurrència en forma matricial de la forma:

$$\left(\frac{PR_{k+1}}{1}\right) = \left(\begin{array}{c|c} (1-p)M & pPR_0 \\ \hline 0 & 1 \end{array}\right) \cdot \left(\frac{PR_k}{1}\right) =: Iterar \cdot \left(\frac{PR_k}{1}\right)$$

és fàcil demostrar que $Iterar$ té 1 com a valor propi i un vector propi de $Iterar$ te algun coeficient no nul en les primeres n coordenades, i tot altre valor propi λ d'$Iterar$ compleix $|\lambda| < 1$ i $dim(ker(Iterar - I_{n+1})) = 1$, per tant fent $PR_N := Iterar^N(PR_0) \sim v$ on v suma $n+1$ i v és vector propi de valor propi 1 de $Iterar$ (on té tots coeficients positius o zeros, es pot demostrar), on aquest últim pas està relacionat amb el teorema de Peron-Frobenius.

Anem a fer aquest algoritme explicit en l'exemple de 4 pàgines web anterior.

Exemple 3.146. *Fem $p = 0,15$, tenim que la matriu amb ordre triat de les webs:A,B,C i D, obtenim*

$$M = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 1/2 & 0 & 0 & 0 \\ 1/2 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

i calculant $PR_k = pPR_0 + (1-p)MPR_{k-1}$ obtenim la taula:

Iteració	*PR(A)*	*PR(B)*	*PR(C)*	*PR(D)*	PR_k
0	*1*	*1*	*1*	*1*	*(1,1,1,1)*
1	*1*	*0.575*	*2.275*	*0.15*	*(1,0.575,2.275,0.150)*
2	*2.084*	*0.575*	*1.191*	*0.15*	
3	*1.163*	*1.036*	*1.652*	*0.15*	
⋮	⋮	⋮	⋮	⋮	
15	*1.491*	*0.783*	*1.576*	*0.150*	
16	*1.490*	*0.783*	*1.577*	*0.150*	
17	*1.490*	*0.783*	*1.577*	*0.150*	

i estabilitza, per tant ordenaria: C, A, B i D en aquest ordre.

Bibliografia

[Aig07] Aigner, Martin: Discrete Mathematics. Translated from the 2004 German original by David Kramer. American Mathematical Society, Providence, RI, 2007. xii+388 pp. ISBN: 978-0-8218-4151-8.

[TheBook] Aigner, Martin; Ziegler, Günter M.: Proofs from The Book. Including illustrations by Karl H. Hofmann. Second edition. Springer-Verlag, Berlin, 2001. viii+215 pp. ISBN: 3-540-67865-4.

[BRV07] Basart, J.M, Rifà, J i Villanueva, M.: "Fonaments de matemàtica discreta. Elements de combinatòria i d'aritmètica". Col. Materials de la UAB, n. 36. 1997.

[Ba98] Basart, J.M. "Grafs: fonaments i algoritmes", Col. Manuals de la UAB, n. 13, 1998.

[BoMu08] Bondy, J. A.; Murty, U. S. R. Graph theory. Graduate Texts in Mathematics, 244. Springer, New York, 2008. xii+651 pp. ISBN: 978-1-84628-969-9

[CFSS01] Comellas, F, Fàbrega,J., Sànchez, A, Serra, O. "Matemática discreta". Edicions UPC, 2001.

[Con23] Conrad, Keit, "Equivalence of absolute values". `https://kconrad.math.uconn.edu/blurbs/gradnumthy/equivabsvalues.pdf`.

[GMRV98] Gimbert, J. Moreno, R., Ribó, J.M., Valls, M. "Apropament a la teoria de grafs i als seus algoritmes". UdL, 1998.

[GoRo01] Godsil, C. D; Royle, G. "Algebraic graph theory" GTM, Springer, 2001.

[Ko84] Koblitz, Neal. "P-adic numbers, p-adic analysis, and zeta-functions". Graduate Texts in Mathematics (2nd ed.). New York: Springer-Verlag (1984). ISBN 978-0-387-96017-3.

[Vo93] Voigt, Margit.: List colourings of planar graphs. Discrete Math. 120 (1993), no. 1-3, 215–219.