Matemàtica Discreta

Biel Cardona

24 de setembre de 2013

Índex

Tema 1

Lògica i fonamentació

Lliçó 1

Lògica proposicional

1.1 Proposicions i connectors

Tot i que fonamentar-ho de manera precisa ens portaria molta feina, podríem dir que una *proposició lògica* és una sentència que pot ser (o ser considerada) *certa* o *falsa*, independentment de qualsevol consideració. Així "dos i dos són quatre" o "tres i tres són vuit" són proposicions, mentre que "quants són dos i dos?" o "un nombre parell" no ho són.

Sovint s'indicaran les proposicions per lletres minúscules ($p, q, r, \ldots$), que podem entendre com a variables que poden prendre dos valors: 1 (o V) per a cert i 0 (o F) per a fals.

Les proposicions es poden composar per formar-ne d'altres per mitjà de *connectors lògics*:

- Negació: $\neg p$ és la proposició que pren el valor V exactament quan p pren el valor F. En el llenguatge habitual, la negació d'una proposició p s'expressa com "no p" o "p és fals".
- Conjunció: $p \wedge q$ és la proposició que pren el valor V exactament quan totes dues proposicions prenen el valor V, i el valor F quan almenys una de les dues pren el valor F. En el llenguatge habitual, la proposició $p \wedge q$ s'expressa com "p i q".
- Disjunció: $p \vee q$ és la proposició que pren el valor V quan almenys una de les proposicions p o q pren el valor V, i el valor F quan totes dues prenen el valor F. En el llenguatge habitual, la proposició $p \vee q$ s'expressa com "p o q".
- Disjunció exclusiva: $p \oplus q$ pren el valor V quan una i només una de les proposicions que la formen pren el valor V.
- Implicació: $p \to q$ pren el valor F quan p (l'*antecedent*) pren el valor V i q (el *conseqüent*) pren el valor F; altrament pren el valor V. En el llenguatge habitual, la proposició $p \to q$ s'expressa de moltes formes diferents: "Si p, aleshores q"; "p implica q"; "p és suficient per q"; "q és necessari per p"; "sempre que p es té q";...
- Doble implicació: $p \leftrightarrow q$ pren el valor V quan totes dues proposicions prenen el mateix valor; altrament pren el valor F. Aquesta proposició s'expressa habitualment com: "p i q són equivalents"; "p si, i només si, q" (que sovint s'escursa com "p ssi q"); "p és necessari i suficient per a q";...

Una proposició que no es pot descomposar en altres lligades per connectors lògics s'anomena *proposició atòmica*.

Exemple: Considerem la sentència "Si avui és diumenge i no plou, aniré al futbol". Podem considerar que està formada per 3 proposicions atòmiques, "avui és diumenge" (que indicarem per p), "avui plou" (que indicarem per q) i "aniré al futbol" (que indicarem per r). Aleshores la sentència anterior la podem escriure com

$$(p \wedge \neg q) \rightarrow r.$$

Considerem diferents situacions i el valor que pren la sentència:

- Avui és diumenge, no plou i vaig al futbol: és a dir, $p = \mathrm{V}, q = \mathrm{F}, r = \mathrm{V}$. Aleshores $(p \wedge \neg q) = \mathrm{V}$ i per tant la sentència de l'enunciat és certa, ja que $\mathrm{V} \rightarrow \mathrm{V} = \mathrm{V}$.
- Avui és dissabte, plou i vaig al futbol: és a dir, $p = \mathrm{F}, q = \mathrm{V}, r = \mathrm{V}$. Aleshores $(p \wedge \neg q) = \mathrm{F}$ i per tant la sentència de l'enunciat és certa, ja que $\mathrm{F} \rightarrow \mathrm{V} = \mathrm{V}$.
- Avui és dijous, no plou i no vaig al futbol: és a dir, $p = \mathrm{F}, q = \mathrm{F}, r = \mathrm{F}$. Aleshores $(p \wedge \neg q) = \mathrm{F}$ i per tant la sentència de l'enunciat és certa, ja que $\mathrm{F} \rightarrow \mathrm{F} = \mathrm{V}$.
- Avui és diumenge, no plou i no vaig al futbol: és a dir, $p = \mathrm{V}, q = \mathrm{F}, r = \mathrm{F}$. Aleshores $(p \wedge \neg q) = \mathrm{V}$ i per tant la sentència de l'enunciat és falsa, ja que $\mathrm{V} \rightarrow \mathrm{F} = \mathrm{F}$.

De manera anàloga que amb les operacions amb enters, els diferents connectors lògics venen donats amb diferents precedències, per tal d'estalviar-se l'ús excessiu de parèntesis. Així, l'ordre de major a menor precedència entre ells és:

- $\neg$
- $\wedge$,$\vee$
- $\rightarrow$
- $\leftrightarrow$

Exemple: La proposició $\neg p \vee q \rightarrow r$ s'ha de llegir com $((\neg p) \vee q) \rightarrow r$.

Una manera d'expressar els valors lògics V o F que pren una proposició composada en funció de les seves parts integrants és mitjançant *taules de veritat* on es posa una fila per a cada possible assignació de valor a cadascuna de les proposicions elementals que hi apareixen.

p	$\neg p$
0	1
1	0

p	q	$p \wedge q$
0	0	0
0	1	0
1	0	0
1	1	1

p	q	$p \vee q$
0	0	0
0	1	1
1	0	1
1	1	1

p	q	$p \oplus q$
0	0	0
0	1	1
1	0	1
1	1	0

p	q	$p \rightarrow q$
0	0	1
0	1	1
1	0	0
1	1	1

p	q	$p \leftrightarrow q$
0	0	1
0	1	0
1	0	0
1	1	1

Exemple: Considerem la proposició $(p \wedge q) \vee r \leftrightarrow s$. La seva taula de veritat és

p	q	r	s	$(p \wedge q)$	$(p \wedge q) \vee r$	$(p \wedge q) \vee r \leftrightarrow s$
0	0	0	0	0	0	1
0	0	0	1	0	0	0
0	0	1	0	0	1	0
0	0	1	1	0	1	1
0	1	0	0	0	0	1
0	1	0	1	0	0	0
0	1	1	0	0	1	0
0	1	1	1	0	1	1
1	0	0	0	0	0	1
1	0	0	1	0	0	0
1	0	1	0	0	1	0
1	0	1	1	0	1	1
1	1	0	0	1	1	0
1	1	0	1	1	1	1
1	1	1	0	1	1	0
1	1	1	1	1	1	1

1.2 Equivalència

Observem que els connectors introduïts no són independents; es a dir, es poden posar uns en funció dels altres. Per exemple, $p \rightarrow q$ i $(\neg p) \vee q$ prenen els mateixos valors sigui quina sigui l'assignació de valors a p i q. En aquest cas es diu que les proposicions donades són *lògicament equivalents*, i s'indica amb el símbol $\iff$. Així, per indicar que $p \rightarrow q$ i $(\neg p) \vee q$ són equivalents, posem

$$p \rightarrow q \iff \neg p \vee q$$

Una *tautologia* és una proposició que pren sempre el valor V, sigui quina sigui l'assignació de valors lògics a les seves proposicions atòmiques. Per exemple, $p \vee \neg p$ és una tautologia.

Per contra, una *contradicció* és una proposició que pren sempre el valor F. Per exemple, $p \wedge \neg p$ és una contradicció.

Una forma d'expressar que p i q són equivalents és dir que $p \leftrightarrow q$ és una tautologia.

Del concepte d'equivalència en deriven les *lleis lògiques* següents:

- Lleis d'identitat:

$$p \wedge \mathrm{V} \iff p$$
$$p \vee \mathrm{F} \iff p$$

- Lleis de dominació:

$$p \wedge \mathrm{F} \iff \mathrm{F}$$
$$p \vee \mathrm{V} \iff \mathrm{V}$$

- Lleis d'idempotència:

$$p \wedge p \iff p$$
$$p \vee p \iff p$$

- Llei de doble negació:
$$\neg(\neg p) \iff p$$
- Lleis commutatives:
$$p \wedge q \iff q \wedge p$$
$$p \vee q \iff q \vee p$$
- Lleis associatives:
$$p \wedge (q \wedge r) \iff (p \wedge q) \wedge r$$
$$p \vee (q \vee r) \iff (p \vee q) \vee r$$
- Lleis de De Morgan:
$$\neg(p \wedge q) \iff \neg p \vee \neg q$$
$$\neg(p \vee q) \iff \neg p \wedge \neg q$$
- Lleis de la tautologia i la contradicció
$$p \vee \neg p \iff \mathrm{V}$$
$$p \wedge \neg p \iff \mathrm{F}$$
- Llei de la implicació:
$$p \to q \iff \neg p \vee q \iff \neg(p \wedge \neg q)$$

Aquestes equivalències es poden provar fàcilment fent servir taules de veritat, tot i que és més important entendre que reflecteixen els raonaments lògics habituals.

Exemple:

- Si diem "És fals que avui sigui diumenge i plogui", estarem dient la veritat exactament quan o bé no és diumenge, o bé no plou, o bé totes dues coses. Això és essencialment el que diu la llei de De Morgan.
- Si diem "Si avui és diumenge, aleshores aniré a passejar", la única forma possible en que el que diem és fals és que sigui diumenge i no anem a passejar. Dit d'altre forma, estarem dient una veritat exactament quan no sigui diumenge o quan vagi a passejar.

Lliçó 2

Lògica de primer ordre

2.1 Predicats

La lògica de primer ordre (o predicativa) estén la proposicional admetent que el valor que prenen les "proposicions" depengui de variables.

Així, una forma proposicional de primer ordre està formada per *variables* i *predicats* que estableixen propietats o relacions entre les variables. Per exemple, "x és parell" és una funció proposicional amb la variable x i el predicat "ser parell". Les funcions proposicionals esdevenen proposicions per assignació de variables a valors concrets. Sovint s'indica per lletres majúscules les funcions proposicionals, indicant entre parèntesi les variables que contenen, i sovint s'anomenen simplement predicats, en el benentès que les variables formen part seva. Per exemple, $P(x), Q(x, y)$ indiquen predicats amb, respectivament, una i dues variables.

2.2 Quantificadors

Sovint es vol expressar quins valors lògics pren un predicat quan les variables prenen diferents possibilitats.

El *quantificador universal* tradueix al llenguatge lògic una expressió del tipus "per a tot x es té $P(x)$", significant que sigui quina sigui l'assignació de la variable x (entre un determinat univers Ω de possibilitats), el predicat P pren el valor V. Aquest quantificador s'indica amb el símbol $\forall$, de manera que l'expressió anterior s'escriu

$$(\forall x \in \Omega)P(x) \qquad \text{o} \qquad \forall x[P(x)] \qquad \text{o} \qquad \forall x P(x).$$

El *quantificador existencial* tradueix una expressió del tipus "existeix algun x tal que $P(x)$", significant que hi ha almenys una assignació de valor a x de manera que el predicat P pren el valor V. Aquest quantificador s'indica amb el símbol $\exists$, de manera que l'expressió anterior s'escriu

$$(\exists x \in \Omega)P(x) \qquad \text{o} \qquad \exists x[P(x)] \qquad \text{o} \qquad \exists x P(x).$$

Una variant del quantificador existencial és el *quantificador existencial amb unicitat*, que tradueix expressions del tipus "existeix un únic x tal que $P(x)$". Aquest s'indica substituint el símbol $\exists$ per $\exists!$, i es pot expressar com:

$$(\exists! x)P(x) \iff \exists x P(x) \wedge (\forall x \forall y)[(P(x) \wedge P(y)) \to (x = y)],$$

és a dir, existeix un tal x i si dos elements compleixen la propietat, necessàriament són iguals.

Observem que, en quantificar un predicat, de manera que totes les variables que apareixen es quantifiquin, obtenim una proposició, que pot ser certa o falsa.

Exemple: Considerem el predicat "x és un nombre parell", on l'univers que es considera és el dels nombres enters, i que indiquem per $P(x)$. Aleshores la proposició $(\exists x)P(x)$ és certa, ja que podem considerar l'enter 2, que és parell. En canvi, la proposició $(\forall x)P(x)$ és falsa, ja que, per exemple, l'enter 3 no és parell.

Si l'univers al que fa referència un determinat predicat és finit, és a dir, x pot prendre un conjunt finit de valors $x_1, \ldots, x_n$, la proposició $\forall x P(x)$ es pot escriure com

$$P(x_1) \wedge P(x_2) \wedge \cdots \wedge P(x_n),$$

i la proposició $\exists x P(x)$ com

$$P(x_1) \vee P(x_2) \vee \cdots \vee P(x_n).$$

Cal tenir en compte que si l'univers d'aplicació es buit, tota proposició quantificada universalment és certa, mentre que tota proposició quantificada existencialment és falsa.

Quan apareixen diverses variables amb diferents quantificadors, l'ordre en que apareixen és important. Per exemple, la proposició

$$\exists x \forall y P(x, y)$$

s'ha d'entendre com

$$\exists x[\forall y P(x, y)].$$

Així, $\forall y P(x, y)$ és un predicat en la variable x, i la proposició s'obté al aplicar-hi un quantificador existencial a aquest predicat. La traducció al llenguatge corrent d'aquesta proposició és "existeix un x tal que per a tot y es té $P(x, y)$". Per altra banda, la proposició

$$\forall y \exists x P(x, y)$$

s'ha d'entendre com

$$\forall y[\exists x P(x, y)].$$

Ara, $\exists x P(x, y)$ és un predicat en la variable y que, al aplicar-hi el quantificador existencial esdevé una proposició. La traducció al llenguatge corrent d'aquesta és "per a tot y existeix un x (que pot dependre de y) de manera que $P(x, y)$".

Exemple: Considerem com a univers els nombres reals, i sigui $P(x, y)$ el predicat "$x + y = 0$". Aleshores, $\forall y \exists x P(x, y)$ es tradueix en dir que tot nombre real té un invers respecte de la suma, cosa que és certa. En canvi, $\exists x \forall y P(x, y)$ es tradueix en dir que existeix un nombre real que, sumant-li el nombre que li sumem, dóna sempre 0, cosa que és falsa.

Com a totes les proposicions, les que s'obtenen per quantificació de predicats es poden composar; específicament, la negació d'un quantificador existencial és un quantificador universal, i viceversa. Així,

$$\neg(\forall x P(x)) \iff \exists x(\neg P(x)),$$
$$\neg(\exists x P(x)) \iff \forall x(\neg P(x)).$$

2.3 Regles d'inferència i raonaments

El raonament matemàtic es basa en el concepte de *demostració*; és a dir, partir de certs resultats que se suposen certs per tal de decidir (o refutar) la certesa d'altres. La fonamentació rigorosa de les demostracions prové de les *regles d'inferència*. Per exemple (modus ponens): Si suposem certa la proposició $p \to q$ i també la proposició p, aleshores deduïm que la proposició q és certa. Això s'indica en el llenguatge de la lògica com:

$$\begin{array}{l} p \to q \\ p \\ \hline \therefore \quad q \end{array}$$

i es pot formular en termes de lògica proposicional dient que

$$((p \to q) \wedge p) \to q$$

és una tautologia.

Les regles d'inferència més habituals són:

- Addició:
$$\begin{array}{l} p \\ \hline \therefore \quad p \vee q \end{array}$$
- Simplificació:
$$\begin{array}{l} p \wedge q \\ \hline \therefore \quad p \end{array}$$
- Conjunció:
$$\begin{array}{l} p \\ q \\ \hline \therefore \quad p \wedge q \end{array}$$
- Modus ponens:
$$\begin{array}{l} p \to q \\ p \\ \hline \therefore \quad q \end{array}$$
- Modus tollens:
$$\begin{array}{l} p \to q \\ \neg q \\ \hline \therefore \quad \neg p \end{array}$$
- Sil·logisme hipotètic:
$$\begin{array}{l} p \to q \\ q \to r \\ \hline \therefore \quad p \to r \end{array}$$
- Sil·logisme disjuntiu:
$$\begin{array}{l} p \vee q \\ \neg q \\ \hline \therefore \quad p \end{array}$$

Exemple:

- Suposem que la sentència "si avui és diumenge, aniré al futbol" és certa. En aquest cas, si és diumenge, puc deduir que vaig al futbol (Modus Ponens). Si no vaig al futbol, puc deduir que no és diumenge (Modus Tollens).
- Suposem que la sentència "tinc gana o tinc set" és certa. Si, a més, sé que no tinc set, puc deduir que tinc gana (sil·logisme disjuntiu)

Així, un *raonament vàlid* consisteix en una cadena d'aplicació de regles d'inferència que obtenen per resultat la proposició a demostrar.

Les regles d'inferència que hem vist fan referència a la lògica proposicional. Sovint, però, els resultats a provar es descriuen en termes de lògica de primer ordre. En aquest cas, també existeixen regles d'inferència. Per exemple, si suposem certa la proposició $\forall x P(x)$ i c és un element de l'univers de referència, obtenim la certesa de la proposició $P(c)$. Les regles d'inferència en lògica de primer ordre són essencialment dues, amb les variants existencial i universal:

- Particularització universal:
$$\frac{\forall x P(x)}{\therefore \quad P(c)}$$
- Generalització universal:
$$\frac{P(c) \text{ per a } c \text{ arbitrari}}{\therefore \quad \forall x P(x)}$$
- Particularització existencial:
$$\frac{\exists x P(x)}{\therefore \quad P(c) \text{ per a algun } c}$$
- Generalització existencial:
$$\frac{P(c) \text{ per a algun } c}{\therefore \quad \exists x P(x)}$$

Tema 2

Teoria de conjunts

Lliçó 3

Conjunts

3.1 Conjunts i elements

Tot i que (un altre cop) fonamentar exhaustivament el concepte modern de conjunt ens portaria massa feina, entendrem per *conjunt* un objecte matemàtic del que té sentit demanar si un determinat *element* hi pertany o no.

Així, escriurem

$$x \in A$$

per indicar que l'element x pertany al conjunt A, i escriurem

$$x \notin A$$

per indicar el contrari.

Els conjunts es poden descriure de moltes diverses formes; són les més habituals:

- Per enumeració dels seus elements. La forma genèrica d'aquesta descripció és

  $$A = \{a_1, a_2, \ldots, a_n\}.$$

  Atès que únicament podem demanar si un determinat element hi pertany o no, ni l'ordre en que apareixen els elements ni el nombre de vegades que apareix cadascun d'ells té cap rellevància.

- Per propietats definitòries dels seus elements. La forma genèrica d'aquesta descripció és:

  $$A = \{x \mid P(x)\},$$

  indicant que els elements de A són aquells que fan prendre el valor V al predicat $P(x)$.

- Per operacions amb altres conjunts, que veurem més endavant.

Exemple: Són conjunts:

- $A = \{1, 2, 3, 4\}$,
- $B = \{n \mid n \text{ és un enter parell i major que } 1\} = \{2, 4, 6, 8, \ldots\}$,
- C és el conjunt de les paraules catalanes que apareixen al Pompeu-Fabra.

Alguns conjunts que farem servir habitualment són:

- El conjunt dels nombres naturals: $\mathbb{N} = \{0, 1, 2, \dots\}$.
- El conjunt dels nombres enters: $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$.
- L'interval enter de mida n: $[n] = \{1, \dots, n\}$.

Un conjunt sense elements, és a dir, aquell que $x \in A$ és sempre fals, s'anomena el *conjunt buit*, i s'indica per $\emptyset = \{\}$. Un conjunt amb un únic element es diu que és un *singletó*.

Dos conjunts A i B direm que són *iguals* si tenen el mateixos elements, i ho indicarem per $A = B$. En termes lògics, es pot descriure que dos conjunts són iguals per:

$$A = B \iff \forall x \left[(x \in A) \leftrightarrow (x \in B)\right].$$

Direm que A és un *subconjunt* de B, i ho indicarem per $A \subseteq B$ ó $B \supseteq A$ si tot element de A també ho és de B, és a dir:

$$A \subseteq B \iff \forall x \left[(x \in A) \rightarrow (x \in B)\right].$$

Si, a més, $A \neq B$, direm que A és un subconjunt *propi* de B, i ho indicarem per $A \subsetneq B$ o simplement per $A \subset B$. No confonguem aquest amb $A \not\subseteq B$, que vol dir que és fals que $A \subseteq B$, és a dir, que existeix almenys un element de A que no pertany a B.

De la definició donada es segueix trivialment que el conjunt buit és subconjunt de qualsevol conjunt, i que

$$A = B \iff (A \subseteq B \wedge B \subseteq A).$$

De fet, aquesta identitat és sovint emprada per a demostrar la igualtat de conjunts.

Exemple: Considerem els conjunts:

- $A = \{n \mid \ n \text{ és un enter parell}\}$,
- $B = \{n \mid \ n \text{ és un enter múltiple de } 4\}$,
- $C = \{n \mid \ n \text{ és un enter i } (-1)^n = 1\}$.

Aleshores:

$$B \subset A, \qquad A = C$$

Dos conjunts A i B direm que són *equipotents*, i ho indicarem per $A \sim B$, si es pot donar una bijecció (correspondència 1 a 1) entre els seus elements. Direm també que A i B tenen el mateix *cardinal*, o tenen el mateix *nombre d'elements*, i ho indicarem per $|A| = |B|$.

Un conjunt es diu que és *infinit* si és equipotent a algun subconjunt propi seu; altrament direm que és *finit*. Tot i aquesta definició formal, els conjunts finits són aquells equipotents a algun de la forma $\{1, \dots, n\}$ amb n un enter positiu, que és també el seu cardinal.

3.2 Operacions amb conjunts

La *intersecció* de dos conjunts A i B, que indiquem per $A \cap B$, és el conjunt format pels elements que pertanyen tant a A com a B,

$$A \cap B = \{x \mid (x \in A) \wedge (x \in B)\}.$$

Recursivament, es pot definir la intersecció d'una família finita de conjunts, i en general es pot definir la intersecció d'una família arbitrària de conjunts A_i indexada per un conjunt no buit I com

$$\bigcap_{i \in I} A_i = \{x \mid x \in A_i \text{ per a tot } i \in I\}.$$

La *unió* de dos conjunts A i B, que indiquem per $A \cup B$, és el conjunt format pels elements que pertanyen a almenys un d'ells,

$$A \cup B = \{x \mid (x \in A) \vee (x \in B)\}.$$

Anàlogament al cas de la intersecció, es pot definir la unió d'una família arbitrària de conjunts,

$$\bigcup_{i \in I} A_i = \{x \mid x \in A_i \text{ per a algun } i \in I\}.$$

Es diu que un conjunt X és la *unió disjunta* d'altres dos conjunts A i B, i s'indica per $X = A \sqcup B$, si $X = A \cup B$ i $A \cap B = \emptyset$. Anàlogament es defineix la unió disjunta d'una família arbitrària $\{A_i\}_{i \in I}$ de conjunts quan aquests són disjunts 2 a 2, és a dir, si $A_i \cap A_j = \emptyset$ per a $i \neq j$.

El *complement* d'un conjunt A (dins un univers Ω que el context deixa clar), que indiquem per $\overline{A}$, és el conjunt format pels elements d'aquest univers que no pertanyen a A,

$$\overline{A} = \{x \mid x \notin A\}.$$

La *diferència* de dos conjunts és

$$A \setminus B = \{x \mid (x \in A) \wedge (x \notin B)\},$$

mentre que la *diferència simètrica* és

$$A \triangle B = (A \setminus B) \cup (B \setminus A).$$

El *producte cartesià* de dos conjunts A i B, que s'indica per $A \times B$ és el conjunt que té per elements parells ordenats d'elements, el primer pertanyent a A i el segon pertanyent a B,

$$A \times B = \{(x, y) \mid x \in A, y \in B\}.$$

Recursivament, això permet definir el producte cartesià

$$A_1 \times A_2 \times \cdots \times A_n = \{(x_1, x_2, \ldots, x_n) \mid x_i \in A_i \text{ per a tot } i\}.$$

En el cas que els conjunts que fem el producte cartesià són el mateix, s'indica per

$$A^n = A \times A \times \cdots \times A.$$

El *conjunt de parts* d'un conjunt A és el conjunt que té per elements els subconjunts de A,

$$\mathcal{P}(A) = \{B \mid B \subseteq A\}.$$

Notem que sigui quin sigui A, $\mathcal{P}(A)$ té almenys dos elements, $\emptyset$ i A, que poden ser iguals en el cas que $A = \emptyset$.

Exemple: Prenguem $A = \{1, 2, 3, 4\}$ i $B = \{2, 3, 5, 7\}$, on suposem que l'univers de referència és el conjunt de nombres naturals. Aleshores:

- $A \cup B = \{1, 2, 3, 4, 5, 7\}$
- $A \cap B = \{2, 3\}$
- $\overline{A} = \{n \in \mathbb{N} \mid n > 4\}$
- $A \setminus B = \{1, 4\}$
- $A \triangle B = \{1, 4, 5, 7\}$
- $A \times B = \{(1,2), (1,3), (1,5), (1,7), (2,2), (2,3), (2,5), (2,7), (3,2), (3,3), (3,5), (3,7), (4,2), (4,3), (4,5), (4,7)\}$
- $\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{1,4\}, \{2,3\}, \{2,4\}, \{3,4\}, \{1,2,3\}, \{1,2,4\}, \{1,3,4\}, \{2,3,4\}, \{1,2,3,4\}\}$

Una família $\{A_i\}_{i \in I}$ de subconjunts d'un conjunt A es diu que forma una *partició* de A si tot element de A pertany a un i només un subconjunt de la família. Equivalentment, si $\cup_{i \in I} A_i = A$ i $A_i \cap A_j = \emptyset$ per a tot $i \neq j$.

Una partició $\{A_i\}_{i \in I}$ es diu que *refina* una altra partició $\{B_j\}_{j \in J}$ si tot subconjunt A_i de la primera és subconjunt d'algun B_j de la segona.

Exemple: Considerem $X = \{1, \ldots, 10\}$. Les famílies:

$$A_1 = \{1, 3, 5, 7, 9\}, \qquad A_2 = \{2, 4, 6, 8, 10\}$$

i

$$B_1 = \{1, 5\}, \qquad B_2 = \{3, 7\}, \qquad B_3 = \{9\}, \qquad B_4 = \{2, 4, 6, 8, 10\}$$

són particions de X, i la partició $\{B_i\}$ és un refinament de la partició $\{A_i\}$.

Les lleis d'equivalència de la lògica proposicional tenen el seu equivalent en teoria de conjunts:

- Lleis d'identitat:

$$A \cap \Omega = A$$

$$A \cup \emptyset = A$$

- Lleis de dominació:

$$A \cap \emptyset = \emptyset$$

$$A \cup \Omega = \Omega$$

- Lleis d'idempotència:

$$A \cap A = A$$

$$A \cup A = A$$

- Llei de doble complement:

$$\overline{\overline{A}} = A$$

- Lleis commutatives:

$$A \cap B = B \cap A$$
$$A \cup B = B \cup A$$

- Lleis associatives:

$$A \cap (B \cap C) = (A \cap B) \cap C$$
$$A \cup (B \cup C) = (A \cup B) \cup C$$

- Lleis de De Morgan:

$$\overline{A \cap B} = \overline{A} \cup \overline{B}$$
$$\overline{A \cup B} = \overline{A} \cap \overline{B}$$

- Lleis del tercer exclòs:

$$A \cap \overline{A} = \emptyset$$
$$A \cup \overline{A} = \Omega$$

Lliçó 4

Multiconjunts

Sovint és interessant considerar conjunts on els seus elements puguin aparèixer un nombre determinat de cops. Així, un *multiconjunt* es pot pensar com un conjunt A on cada element $a \in A$ apareix un nombre $m_A(a) > 0$ de vegades. Per simetria, es defineix $m_A(a) = 0$ si $a \notin A$. Els multiconjunts s'indiquen fent servir les mateixes notacions de conjunts.

Exemple: Considerem el multiconjunt $A = \{1, 1, 1, 2, 2, 4, 5, 5\}$, on la multiplicitat que apareix en la descripció és la seva multiplicitat en el multiconjunt. Aleshores:

$$m_A(1) = 3, \quad m_A(2) = 2, \quad m_A(3) = 0, \quad m_A(4) = 1, \quad m_A(5) = 2.$$

Els conceptes d'igualtat i inclusió de multiconjunts es defineixen com en el cas dels conjunts, tenint en compte que s'han de respectar les multiplicitats:

$$A = B \iff \forall x[m_A(x) = m_B(x)]$$
$$A \subseteq B \iff \forall x[m_A(x) \leqslant m_B(x)]$$

La unió i intersecció de multiconjunts es defineix també imitant les propietats dels conjunts; si A i B són multiconjunts, el multiconjunts $A \cup B$ i $A \cap B$ venen determinats per

$$m_{A \cup B}(x) = \max(m_A(x), m_B(x)),$$
$$m_{A \cap B}(x) = \min(m_A(x), m_B(x)),$$

on max i min indiquen, respectivament el màxim i el mínim dels seus arguments. Anàlogament, la diferència de dos multiconjunts s'obté descomptant al primer els elements del segon amb la multiplicitat corresponent:

$$m_{A \setminus B}(x) = \max(0, m_A(x) - m_B(x)).$$

El concepte de cardinal d'un conjunt s'estén a multiconjunts de manera òbvia, és a dir, cada element contribueix al cardinal del multiconjunt amb tantes unitats com la seva multiplicitat, cosa que podem expressar com $|A| = \sum_{a \in A} m_A(a)$.

Exemple: Considerem els multiconjunts

$$A = \{1, 1, 1, 2, 2, 4, 5, 5\}, \qquad B = \{1, 2, 2, 2, 2, 3, 3, 5, 5, 7\}.$$

Aleshores

$$\begin{aligned} A \cup B &= \{1, 1, 1, 2, 2, 2, 2, 3, 3, 4, 5, 5, 7\} \\ A \cap B &= \{1, 2, 2, 5, 5\} \\ A \setminus B &= \{1, 1, 4\} \\ |A| &= 8 \\ |B| &= 10 \\ |A \cup B| &= 13 \\ |A \cap B| &= 5 \end{aligned}$$

Lliçó 5

Relacions

5.1 Relacions

Una *relació* entre dos conjunts A i B (eventualment iguals) és un subconjunt del seu producte cartesià, $R \subseteq A \times B$. Direm que dos elements $a \in A$ i $b \in B$ estan *relacionats* per R, i ho indicarem per $a\ R\ b$ si $(a, b) \in R$; altrament ho indicarem per $a \not R\ b$.

Les relacions d'un conjunt amb ell mateix poden tenir (o no) les següents propietats:

- Propietat reflexiva: Per a tot a es té $a\ R\ a$.
- Propietat irreflexiva: Per a tot a es té $a \not R\ a$.
- Propietat simètrica: Per a tots a, b es té que si $a\ R\ b$, aleshores $b\ R\ a$.
- Propietat asimètrica: Per a tots a, b es té que si $a\ R\ b$, aleshores $b \not R\ a$.
- Propietat antisimètrica: Per a tots a, b, es té que si $a\ R\ b$ i $b\ R\ a$, aleshores $a = b$.
- Propietat transitiva: Per a tots a, b, c, es té que si $a\ R\ b$ i $b\ R\ c$, aleshores $a\ R\ c$.
- Propietat intransitiva: Per a tots a, b, c, es té que si $a\ R\ b$ i $b\ R\ c$, aleshores $a \not R\ c$.

Exemple: Considerem les relacions següents sobre el conjunt $A = \{1, 2, 3, 4\}$:

$$
\begin{aligned}
R_1 &= \{(1,1),(1,2),(2,1),(2,2),(3,4),(4,1),(4,4)\},\\
R_2 &= \{(1,1),(1,2),(2,1)\},\\
R_3 &= \{(1,1),(1,2),(1,4),(2,1),(2,2),(3,3),(4,1),(4,4)\},\\
R_4 &= \{(2,1),(3,1),(3,2),(4,1),(4,2),(4,3)\},\\
R_5 &= \{(1,1),(1,2),(1,3),(1,4),(2,2),(2,3),(2,4),(3,3),(3,4),(4,4)\},\\
R_6 &= \{(3,4)\}.
\end{aligned}
$$

Aleshores:

- La propietat reflexiva es compleix per a R_3 i R_5.
- La propietat irreflexiva es compleix per a R_4 i R_6.

- La propietat simètrica es compleix per a R_2 i R_3.
- La propietat asimètrica es compleix per a R_4 i R_6.
- La propietat antisimètrica es compleix per a R_4, R_5 i R_6.
- La propietat transitiva es compleix per a R_4, R_5 i R_6.

Observem que, per exemple, la propietat irreflexiva no és la negació de la reflexiva; hi pot haver relacions que no siguin ni reflexives ni irreflexives. Aquesta mateixa observació s'aplica a les propietats simètrica, asimètrica i antisimètrica, així com a la transitiva i intransitiva.

La *clausura* d'una certa relació respecte d'una certa propietat és, cas d'existir, la més petita relació (des d'un punt de vista de teoria de conjunts) que conté la relació donada i compleix la propietat. Equivalentment, correspon a la intersecció (des d'un punt de vista de teoria de conjunts) de la família de relacions que conten la donada i tenen la propietat.

Observem que aquesta família de relacions que contenen una donada i tenen una determinada propietat pot ser buida; aquest és el cas en què no existeix la clausura. Per exemple, si es té una relació sobre un conjunt A i existeix un element $a \in A$ amb $a \; R \; a$, no pot existir la seva clausura irreflexiva, ja que cap relació irreflexiva contindrà la donada.

Una relació entre A i B es pot veure també com una funció (veure la següent lliçó) de A amb imatge $\mathcal{P}(B)$, de manera que a un cert element $a \in A$ se li assigna el conjunt d'elements b de B tals que $a \; R \; b$.

5.2 Relacions d'ordre parcial

Una relació es diu que és un *ordre parcial* si compleix les propietats reflexiva, antisimètrica i transitiva. Habitualment, els ordres s'indiquen amb el símbol $\leqslant$, de manera que es posa $a \leqslant b$ (o $b \geqslant a$) per indicar que els elements estan relacionats, i la notació $a < b$ (o $b > a$) indica que $a \leqslant b$ i $a \neq b$.

Un conjunt on hi ha definit un ordre parcial s'anomena un *conjunt parcialment ordenat* o *poset* (de l'anglès).

Exemple:

- El conjunt de nombres enters (o naturals, racionals i reals) amb l'ordre habitual és un poset.
- El conjunt $\mathbb{Z}$ amb la relació de divisibilitat ($a|b$ si existeix un enter c amb $b = a \cdot c$) és un poset.
- Donat un conjunt A qualsevol, el conjunt de les seves parts $\mathcal{P}(A)$ amb la relació d'inclusió és un poset.

Observem que en un poset no tot parell d'elements és necessàriament comparable, és a dir, poden existir elements a, b amb $a \not\leqslant b$ i $b \not\leqslant a$. Per exemple, a $\mathbb{Z}$ amb l'ordre de divisibilitat, 2 i 3 no són comparables.

Un element a d'un poset $(S, \leqslant)$ es diu que és:

- *minimal* si no hi ha cap element $b \in S$ amb $b < a$,
- *maximal* si no hi ha cap element $b \in S$ amb $b > a$,
- *mínim* si tot element $b \in S$ compleix que $b \geqslant a$,
- *màxim* si tot element $b \in S$ compleix que $b \leqslant a$.

Observem que si un poset té mínim aquest és necessàriament únic i és un element minimal. En canvi, pot haver-hi diferents minimals dins d'un poset; en aquest cas, cap d'ells serà mínim. Observem també que si un poset és finit, aleshores té, al menys, un minimal. Òbviament, les afirmacions simètriques, fent servir màxims i maximals en lloc de mínims i minimals són també certes.

Exemple: Considerem el conjunt $S = \{2, 3, 6, 9, 18\}$ amb la relació de divisibilitat. En aquest poset, 2 i 3 són elements minimals, però no té mínims, mentre que 18 és un màxim, que és el seu únic maximal.

També es diu que un element a d'un poset $(S, \leqslant)$ és:

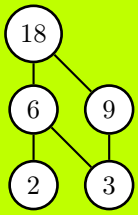
- *fita inferior* d'un subconjunt $T \subseteq S$ si tot element de $b \in T$ compleix que $b \geqslant a$.
- *fita superior* d'un subconjunt $T \subseteq S$ si tot element de $b \in T$ compleix que $b \leqslant a$.
- *ínfim* d'un subconjunt $T \subseteq S$ si és un fita inferior de T i tota fita inferior b de T compleix que $b \leqslant a$. Dit d'altra forma, és un màxim del conjunt de fites inferiors de T.
- *suprem* d'un subconjunt $T \subseteq S$ si és un fita superior dde T i tota fita superior b de T compleix que $b \leqslant a$. Dit d'altra forma, és un mínim del conjunt de fites superiors de T.

Com abans, en cas que un subconjunt T d'un poset S tingui ínfim, aquest és únic i és una fita inferior, però hi pot haver conjunts amb fites inferiors i sense ínfims. I anàlogament per a suprems i fites superiors.

Exemple: Considerem el conjunt $\mathbb{Q}$ dels nombres racionals amb la relació $\leqslant$ habitual. El conjunt $T = \{x \in \mathbb{Q} \mid x \geqslant 0, x^2 \geqslant 2\}$ té fites inferiors, per exemple 0 és una fita inferior; en canvi no té ínfim.

Es diu que un element a d'un poset *cobreix* un altre element b si $a > b$ i no existeix cap element c amb $a > c > b$. El *diagrama de Hasse* d'un poset és el graf (veure el capítol corresponent) que té per vèrtexos els elements del conjunt i s'afegeix un arc de a a b exactament quan a cobreix b. Amb aquesta representació es té que $a \geqslant b$ si, i només si, hi ha un camí sobre el graf que porta de a a b.

Exemple: Per al poset anterior, el seu diagrama de Hasse és el següent:



5.3 Relacions d'equivalència

Una relació es diu que és *d'equivalència* si compleix les propietats reflexiva, simètrica i transitiva. Habitualment les relacions d'equivalència s'indiquen amb el símbol $\sim$ (i també $\simeq, \equiv, =$).

Donada una relació d'equivalència $\sim$ sobre un conjunt A, s'indica per $[a]$ la *classe d'equivalència*,

$$[a] = \{x \in A \mid a \sim x\},$$

i es diu també que a és un *representant* d'aquesta classe.

Dos elements tenen la mateixa classe d'equivalència si, i només si, estan relacionats. En efecte, suposem que $x \sim y$, i sigui $z \in [x]$, és a dir, $x \sim z$; per ser $\sim$ simètrica i transitiva obtenim que $y \sim z$, d'on tenim que $z \in [y]$; per tant obtenim que $[x] \subseteq [y]$ i l'altre inclusió s'obté de la mateixa forma. Recíprocament, si $[x] = [y]$, i com que $x \in [x]$ per la propietat reflexiva, tenim que $x \in [y]$, d'on obtenim que $x \sim y$.

El conjunt format per les classes d'equivalència s'indica per $A/\sim$, i s'anomena el *conjunt quocient* respecte la relació. Aquestes classes d'equivalència formen una partició del conjunt A. En efecte, tot element de A pertany a la seva classe d'equivalència i per tant les classes d'equivalència cobreixen tot el conjunt; per altra banda, si dues classes d'equivalència tenen intersecció no buida, diguem $x \in [a] \cap [b]$, tenim que $x \sim a$ i $x \sim b$, d'on tenim que $[x] = [a]$ i $[x] = [b]$ i, per tant, $[a] = [b]$.

Recíprocament, donada una partició de A, aquesta indueix una relació d'equivalència, dient que dos elements estan relacionats si, i només si, pertanyen al mateix subconjunt de la partició.

Exemple:

- Considerem $\mathbb{Z}$ i fixem un enter N. Dos enters a, b es diuen *congruents mòdul* N, i s'indica per $a \equiv b \pmod{N}$ si $N \mid a - b$. Equivalentment, es pot formular dient que els dos elements proporcionen el mateix residu al fer-ne la divisió euclidiana amb divisor N. La congruència mòdul N és una relació d'equivalència. En aquest cas hi ha N classes d'equivalència, i es poden prendre com a representants d'aquestes els enters $0, \ldots, N-1$. El conjunt quocient s'indica per $\mathbb{Z}_n$ o $\mathbb{Z}/n\mathbb{Z}$, i així es té que $\mathbb{Z}/n\mathbb{Z} = \{[0], [1], \ldots, [n-1]\}$.
- Donada una funció qualsevol $f : A \to B$, definint $a \sim a'$ si, i només si, $f(a) = f(a')$ s'obté una relació d'equivalència sobre A.

Lliçó 6

Funcions

6.1 Definicions

Una *funció* o *aplicació* f d'un conjunt A en un altre conjunt B és una forma d'assignar a cada element de A un únic element de B ben definit, i s'indica per la notació

$$f : A \to B.$$

El conjunt A s'anomena el *domini* (o *abast*) de la funció, B el seu *codomini*. L'element que correspon a un a donat es diu que és la seva *imatge* i s'indica per $f(a)$. Sovint es fa servir la notació

$$a \mapsto f(a)$$

per indicar aquest fet.

El *graf* d'una funció és la relació $\{(a, f(a)) \mid a \in A\} \subseteq A \times B$. És més, es pot definir una funció com una relació on cada element del primer conjunt apareix una i només una vegada a la relació.

El concepte d'imatge es pot estendre a subconjunts; donat $S \subseteq A$, indicarem per $f(S)$ els elements de B que són imatge d'algun element de S, $f(S) = \{f(s) \mid s \in S\}$.

L'*antiimatge* d'un element $b \in B$, $f^{-1}(b)$ és el subconjunt de A format pels elements que tenen b com a imatge, $f^{-1}(b) = \{a \in A \mid f(a) = b\}$. Anàlogament, l'antiimatge d'un subconjunt $T \subseteq B$ està format pels elements de A que tenen imatge dins T, $f^{-1}(T) = \{a \in A \mid f(a) \in T\}$.

El *conjunt imatge* de $f : A \to B$ és el conjunt d'elements que són imatge d'elements de A, és a dir, $f(A)$.

Exemple:

- Funció característica: Donat un conjunt A i un subconjunt seu $B \subseteq A$, s'anomena la *funció característica del subconjunt* B l'aplicació $\chi_B : A \to \{0, 1\}$, determinada per

$$\chi_B(a) = \begin{cases} 1 & \text{si } a \in B \\ 0 & \text{si } a \notin B \end{cases}$$

- Funció modular:

- Donat un enter positiu n, la funció de residu mòdul n, $\mathbb{Z} \to \{0, \ldots, n-1\}$, assigna a cada enter k el residu que resulta en dividir-lo per n, cosa que indiquem per $k \bmod n$.
- L'antiimatge d'un $l \in \{0, \ldots, n-1\}$ qualsevol és el conjunt d'enters $\{\ldots, -2n+l, -n+l, l, n+l, 2n+l, \ldots\}$.
- Dos enters diferents k, k' tenen la mateixa imatge si, i només si, tenen el mateix residu mòdul n; equivalentment, si, i només si, $n \mid k - k'$.

6.2 Propietats

Una funció $f : A \to B$ es diu que és:

- *Injectiva* si elements diferents tenen imatges diferents, és a dir, si $f(a) = f(b)$ implica que $a = b$.
- *Exhaustiva* si tot element del codomini és imatge d'algun element del domini, és a dir, $f(A) = B$.
- *Bijectiva* si és injectiva i exhaustiva.

Donada una funció bijectiva, es considera la *funció inversa* $f^{-1} : B \to A$ que assigna a cada $b \in B$ l'únic $a \in A$ amb $f(a) = b$. Notem que aquest element existeix per la condició d'exhaustivitat i és únic per la injectivitat.

Donades funcions $f : A \to B$ i $g : B \to C$ es defineix la seva *composició* $g \circ f : A \to C$ com $(g \circ f)(a) = g(f(a))$. En el cas que la funció tingui codomini igual al domini es pot composar amb ella mateixa, $f^2 = f \circ f$ i, en general, iterar aquest procés, definint $f^n = f^{n-1} \circ f$.

Fixat un conjunt A, el conjunt de bijeccions de A en A forma un grup, és a dir:

- Compleix la propietat associativa, $f \circ (g \circ h) = (f \circ g) \circ h$;
- Existeix un element neutre, l'aplicació *identitat* $\mathrm{Id}_A : A \to A$ definida per $\mathrm{Id}_A(a) = a$ per a tot $a \in A$;
- Tota funció f té una inversa, f^{-1}, que compleix que $f \circ f^{-1} = f^{-1} \circ f = \mathrm{Id}_A$.

Tema 3

Aritmètica

Lliçó 7

Aritmètica entera bàsica

L'objecte d'estudi en aquesta part és l'anell dels enters:

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}.$$

Diem que formen un *anell* ja que hi ha definides dues operacions, suma $(+)$ i producte $(\cdot)$ que satisfan les propietats:

- Els enters amb la suma formen un *grup abelià*; és a dir, compleixen:
  - Propietat associativa: $a + (b + c) = (a + b) + c$.
  - Element neutre: $a + 0 = 0 + a = a$.
  - Element oposat: $a + (-a) = (-a) + a = 0$.
  - Propietat commutativa: $a + b = b + c$.
- Els enters amb el producte compleixen:
  - Propietat associativa: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
  - Element neutre: $a \cdot 1 = 1 \cdot a = a$.
  - Propietat commutativa: $a \cdot b = b \cdot c$.
- Els enters amb la suma i el producte plegats compleixen:
  - Propietat distributiva: $a \cdot (b + c) = a \cdot b + a \cdot c$.

A banda d'aquestes operacions, sobre els enters tenim definit l'ordre habitual, que dóna estructura a $(\mathbb{Z}, \leqslant)$ de conjunt totalment ordenat:

- És un poset.
- Tot parell d'elements són comparables: o bé $a < b$, o bé $a = b$, o bé $a > b$.

A més, $(\mathbb{Z}, \leqslant)$ compleix la propietat:

- Tot subconjunt no buit $S \subset \mathbb{Z}$ fitat inferiorment té un mínim.

Per acabar, aquesta ordenació és compatible amb les operacions de suma i producte:

- Si $a \leqslant b$, aleshores $a + c \leqslant b + c$ per a tot $c \in \mathbb{Z}$.
- Si $a \leqslant b$, aleshores $a \cdot c \leqslant b \cdot c$ per a tot $c \in \mathbb{N}$.

Teorema 1 (Divisió euclidiana): *Donats $a, b \in \mathbb{Z}$ qualssevol, amb $b \neq 0$, existeixen dos únics enters q (que s'anomena el* quocient*) i r (que s'anomena* resta *o* residu*), amb $0 \leqslant r < |b|$ tals que*

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

Prova: Considerem el conjunt

$$R = \{a - |b|y \mid y \in \mathbb{Z}\} \cap \mathbb{Z}_{\geqslant 0}.$$

Atès que tot element de R és positiu (o zero), R està fitat inferiorment per 0. A més, és no buit, ja que si $a \geqslant 0$, tenim que $a \in R$, mentre que si $a < 0$, $a - |b|a = (1 - |b|)a \in R$. Per tant, existeix un element mínim $r \in R$. A més, per definició de R, tenim que existeix un $y \in \mathbb{Z}$ amb $r = a - |b|y$; si $b > 0$, prenem $q = y$, i altrament $q = -y$, de manera que es compleix que $r = a - b \cdot q$.

Vegem que $0 \leqslant r < |b|$. La primera desigualtat prové de la definició de R. Per a la segona, suposem que $r \geqslant |b|$, i prenem $r' = r - |b|$. Aleshores $r' \in R$ i $r' < r$, contra el fet que r és un mínim de R.

Per a la unicitat, suposem que existeixen altres q', r' amb les propietats demanades. Si $q' = q$, tenim que $r' = r$ i hem acabat. Suposem que $q' < q$; és a dir, $q - q' \geqslant 1$; aleshores,

$$r' = a - |b|q' = (a - |b|q) + |b|(q - q') \geqslant (a - |b|q) + |b| = r + |b| \geqslant |b|,$$

contra la definició de r'; per tant hem arribat a una contradicció. El cas $q' > q$ porta anàlogament a contradicció. Per tant $q = q'$ i $r = r'$. □

Sovint es fa servir la notació $r = a \bmod b$ per indicar el residu que s'obté en fer la divisió euclidiana de a entre b.

Donats enters a i b, diem que a és un *múltiple* de b, o que b és un *divisor* de a, i s'indica per $b \mid a$, si existeix un enter k tal que $a = b \cdot k$; en tal cas, l'enter k s'indica per a/b. La condició que $b \mid a$ és equivalent a que en fer la divisió euclidiana de a entre b s'obtingui residu $a \mod b = 0$.

El conjunt dels enters amb la relació de divisibilitat és un conjunt parcialment ordenat; per tant, si $a|b$ i $b|c$, aleshores $a|c$. A més, la divisibilitat es comporta bé respecta de les operacions bàsiques:

- Si $a|b$ i c és un enter qualsevol, $a|bc$.
- Si $a|b$ i $a|c$, aleshores $a|(b + c)$.

Lliçó 8

Algorisme d'Euclides

Donats enters positius $a, b \in \mathbb{Z}_{>0}$, es defineix el seu *màxim comú divisor* $\mathrm{mcd}(a, b)$ com el més gran d'entre els divisors comuns positius de a i b, i el seu *mínim comú múltiple* com el més petit d'entre els múltiples comuns de a i b. Aquests venen també caracteritzats per les propietats que, per a tot enter x, es té que:

$$a \mid x, \quad b \mid x \implies \mathrm{mcm}(a, b) \mid x,$$
$$x \mid a, \quad x \mid b \implies x \mid \mathrm{mcd}(a, b).$$

Dos enters que tenen màxim comú divisor igual a 1 es diu que són *relativament primers*.

Lema 2: *Siguin $a, b \in \mathbb{Z}_{>0}$ enters positius, i sigui r el residu de la divisió euclidiana $a = bq + r$. Aleshores* $\mathrm{mcd}(a, b) = \mathrm{mcd}(b, r)$.

PROVA: Si d és un divisor comú a a i b, atès que $r = a - bq$, r és també un divisor de r; per tant, d és un divisor comú a b i r. Recíprocament, si d és un divisor comú de b i r, com que $a = bq + r$, també d és un divisor de a; per tant, d és un divisor comú de a i b. Com que a i b, per una banda, i b i r, per l'altra, tenen el mateix conjunt de divisors, tenen també el mateix màxim comú divisor. □

Teorema 3 (Algorisme d'Euclides): *Donats enters positius $a, b \in \mathbb{Z}_{>0}$, posem $r_0 = a$, $r_1 = b$ i considerem la successió de divisions euclidianes:*

$$\begin{aligned}
r_0 &= r_1 q_1 + r_2 && (0 \leqslant r_2 < r_1) \\
r_1 &= r_2 q_3 + r_3 && (0 \leqslant r_3 < r_2) \\
r_2 &= r_3 q_4 + r_4 && (0 \leqslant r_4 < r_3) \\
&\vdots \\
r_{i-1} &= r_i q_{i+1} + r_{i+1} && (0 \leqslant r_{i+1} < r_i) \\
&\vdots \\
r_{k-3} &= r_{k-2} q_{k-1} + r_{k-1} && (0 \leqslant r_{k-1} < r_{k-2}) \\
r_{k-2} &= r_{k-1} q_k + r_k && (r_k = 0)
\end{aligned}$$

Aleshores r_{k-1} (l'últim residu no nul) és igual a $\mathrm{mcd}(a, b)$.

PROVA: Observem que la seqüencia de residus r_i és estrictament decreixent i fitada inferiorment per 0; per tant, en algun moment ha de prendre el valor 0 i l'algorisme acaba.

Pel lema anterior es té que:

$$\mathrm{mcd}(a,b) = \mathrm{mcd}(r_0,r_1) = \mathrm{mcd}(r_1,r_2) = \cdots = \mathrm{mcd}(r_{k-2},r_{k-1}),$$

però com que $r_{k-1} \mid r_{k-2}$, tenim que $\mathrm{mcd}(r_{k-2},r_{k-1}) = r_{k-1}$. □

Exemple: Calculem $\mathrm{mcd}(4864, 3458)$ donant la seqüència de divisions euclidianes que s'obtenen:

i	r	q
0	4864	–
1	3458	–
2	1406	1
3	646	2
4	114	2
5	76	5
6	38	1
7	0	2

Per tant, $\mathrm{mcd}(4864, 3458) = 38$.

Teorema 4 (Algorisme estès d'Euclides — Identitat de Bezout): *Donats enters positius $a, b \in \mathbb{Z}_{>0}$, posem*

$$r_0 = a, \quad x_0 = 1, \quad y_0 = 0,$$
$$r_1 = b, \quad x_1 = 0, \quad y_1 = 1$$

i considerem la successió de divisions euclidianes:

$$\begin{aligned}
r_0 &= r_1q_2 + r_2 & x_2 &= x_0 - q_2x_1, & y_2 &= y_0 - q_2y_1,\\
r_1 &= r_2q_3 + r_3 & x_3 &= x_1 - q_3x_2, & y_3 &= y_1 - q_3y_2,\\
r_2 &= r_3q_4 + r_4 & x_4 &= x_2 - q_4x_3, & y_4 &= y_2 - q_4y_3,\\
&\vdots & & & & \\
r_{i-1} &= r_iq_{i+1} + r_{i+1} & x_{i+1} &= x_{i-1} - q_{i+1}x_i, & y_{i+1} &= y_{i-1} - q_{i+1}y_i,\\
&\vdots & & & & \\
r_{k-3} &= r_{k-2}q_{k-1} + r_{k-1} & x_{k-1} &= x_{k-3} - q_{k-1}x_{k-2}, & y_{k-1} &= y_{k-3} - q_{k-1}y_{k-2},\\
r_{k-2} &= r_{k-1}q_k + r_k & x_k &= x_{k-2} - q_kx_{k-1}, & y_k &= y_{k-2} - q_ky_{k-1},
\end{aligned}$$

Aleshores $x = x_{k-1}$ i $y = y_{k-1}$ compleixen que $\mathrm{mcd}(a,b) = x \cdot a + y \cdot b$.

PROVA: Vegem que a cada pas d'iteració tenim que $r_i = x_ia + y_ib$. En efecte, per a $i = 0, 1$, es compleix trivialment a partir de la definició. Suposem que es compleix per a $i-1$ i per a i, i vegem que també ho fa per a $i+1$:

$$\begin{aligned}
x_{i+1} \cdot a + y_{i+1} \cdot b &= (x_{i-1} - q_{i+1}x_i) \cdot a + (y_{i-1} - q_{i+1}y_i) \cdot b\\
&= (x_{i-1} \cdot a + y_{i-1} \cdot b) - q_{i+1}(x_i \cdot a + y_i \cdot b)\\
&= r_{i-1} - q_{i+1}r_i\\
&= r_{i+1}.
\end{aligned}$$

Per tant, al pas $k-1$, tenim que $\mathrm{mcd}(a,b) = r_{k-1} = x_{i-1}a + y_{i-1}b = x \cdot a + y \cdot b$. □

Aquests càlculs s'expressen de manera senzilla posant una taula de valors, com mostra el següent exemple.

Exemple: Calculem $\mathrm{mcd}(4864, 3458)$ i els coeficients que compleixen la identitat de Bezout.

i	r	q	x	y
0	4864	–	1	0
1	3458	–	0	1
2	1406	1	1	−1
3	646	2	−2	3
4	114	2	5	−7
5	76	5	−27	38
6	38	1	32	−45
7	0	2	−91	128

Per tant, $\mathrm{mcd}(4864, 3458) = 38 = 32 \cdot 4864 + (-45) \cdot 3458$.

Proposició 5: *Fixats enters positius $a, b \in \mathbb{Z}_{>0}$, i un enter arbitrari k, existeixen enters $x, y \in \mathbb{Z}$ tals que $x \cdot a + y \cdot b = k$ si, i només si, k és un múltiple de* $\mathrm{mcd}(a,b)$.

PROVA: Si k és múltiple de $\mathrm{mcd}(a,b)$, diguem $k = k' \cdot \mathrm{mcd}(a,b)$, per la identitat de Bezout tenim que existeixen enters x', y' amb $\mathrm{mcd}(a,b) = x'a + y'b$, d'on $k = k'(x'a + y'b) = (k'x')a + (k'y')b$.

Recíprocament, si k és de la forma $x \cdot a + y \cdot b$, donat d un divisor comú de a i b, es té que d és un divisor de $x \cdot a + y \cdot b$, d'on k és múltiple de d. En particular, k és múltiple de $\mathrm{mcd}(a,b)$. □

Lliçó 9

Nombres primers

Tot i que la manera més habitual de definir els nombres primers és com aquells nombres que no tenen altres divisors que ells mateixos i la unitat, en un contexte més ample, aquest concepte correspon a elements *irreductibles*, mentre que els *primers* són aquells elements que si divideixen un producte, aleshores divideixen algun dels factors. Per sort, en el cas dels nombres enters, aquests dos conceptes coincideixen.

Proposició 6: *Sigui p un enter positiu. Són equivalents:*

1. *Els únics divisors positius de p són 1 i p; és a dir,*

$$p = x \cdot y \implies x = p \text{ ó } y = p.$$

2. *Si p divideix un producte, divideix algun dels factors; és a dir,*

$$p \mid x \cdot y \implies p \mid x \text{ ó } p \mid y.$$

Prova: Suposem que p compleix la segona condició, i sigui $p = x \cdot y$ una factorització seva amb factors positius. Per hipòtesi, tenim que $p \mid x$ ó $p \mid y$; suposem que $p \mid x$. Aleshores $x = pq$ per a cert enter q, i tenim que $p = xy = pqy$, d'on $qy = 1$ i, per tant, $y = 1$ i $x = p$. La suposició que $p \mid y$ ens portaria simètricament a $x = 1$ i $y = p$.

Recíprocament, suposem que p no té divisors positius diferents de 1 i p, i suposem que $p \mid xy$. Si $p \mid x$, ja hem acabat; altrament, tenim que $p \nmid x$ i, com que els únics divisors positius de p són 1 i p, obtenim que $\text{mcd}(p, x) = 1$. Per la identitat de Bezout, siguin $s, t \in \mathbb{Z}$ tals que $1 = sp + tx$. Ara, $y = (sp + tx)y = spy + txy$, d'on $spy = y - txy$. Per tant, $p \mid y - txy$, i com que $p \mid xy$, obtenim que $p \mid y$. □

Proposició 7: *Tot nombre major que 1 es divideix per algun nombre primer.*

Prova: Suposem que el conjunt d'enters majors que 1 que no es divideixen per cap nombre primer és no buit, i sigui n un mínim d'aquest conjunt. Com que n no és primer (ja que n és un divisor de n i, per definició, els divisors de n no són primers), existeix una factorització no trivial $n = ab$, amb $1 < a, b < n$. Ara, a si que es divideix per un nombre primer (n és el més petit amb aquesta propietat), però tot divisor de a ho és també de n. Hem arribat a una contradicció. □

Teorema 8: *Hi ha infinits nombres primers.*

PROVA: Suposem que no, i sigui n una fita superior per als nombres primers. Considerem $m = n! + 1$; aquest nombre no és divisible per cap enter $k \leqslant n$, ja que $m \bmod k = 1 \neq 0$. Per tant, no és divisible per cap nombre primer, cosa que és una contradicció. □

Exemple: Els primers més petits són:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61,\ 67, 71, 73, 79, 83, 89, 97, \ldots$$

Teorema 9 (Fonamental de l'aritmètica): *Els nombres enters tenen factorització única. És a dir, donat un enter no nul, aquest es descomposa de forma única en producte de primers.*

PROVA: Ja hem provat anteriorment que tot nombre descomposa (llevat del signe) en producte de primers. La caracterització donada implica, a més, la unicitat. En efecte, siguin $n = \pm 1 p_1 \cdots p_k = \pm 1 q_1 \cdots q_l$ dues factoritzacions diferents de n; el signe ± 1 queda determinat pel fet que n sigui positiu o negatiu; per tant, és igual en totes dues descomposicions; ara, es té que $p_1 \mid q_1 \cdots q_l$, d'on es té que $p_1 \mid q_i$ (per algun i); per tant, $p_1 = q_i$ i el procés es pot iterar prenent ara n/p_1, per arribar a la igualtat (llevat de l'ordre) en les descomposicions. □

Donat un primer p i un enter n, indicarem per $\mathrm{ord}_p(n)$ el nombre de cops que apreix p en la descomposició en nombres primers de n; dit d'altra forma, $\mathrm{ord}_p(n)$ ve determinat per:

$$p^{\mathrm{ord}_p(n)} \mid n, \qquad p^{\mathrm{ord}_p(n)+1} \nmid n.$$

Òbviament, si $p \nmid n$, posarem $\mathrm{ord}_p(n) = 0$.

Degut a la descomposició única dels enters en producte de primers, tenim que $a \mid b$ si, i només si, $\mathrm{ord}_p(a) \leqslant \mathrm{ord}_p(b)$ per a tot primer p, i d'aquí se'n dedueix que el màxim comú divisor i mínim comú múltiple de dos nombres es pot expressar també per:

$$\mathrm{mcd}(a, b) = \prod_p p^{\min(\mathrm{ord}_p(a), \mathrm{ord}_p(b))},$$

$$\mathrm{mcm}(a, b) = \prod_p p^{\max(\mathrm{ord}_p(a), \mathrm{ord}_p(b))},$$

on el producte s'extén sobre tots els nombres primers, tot i que està clar que únicament un nombre finit d'ells contribuiran al producte. A més, d'aquesta descripció es segueix de forma immediata que $a \cdot b = \mathrm{mcd}(a, b) \cdot \mathrm{mcm}(a, b)$.

Exemple: Seguint amb l'exemple anterior, tenim que $4864 = 2^8 \cdot 19$ i $3458 = 2 \cdot 7 \cdot 13 \cdot 19$. Per tant, $\mathrm{mcd}(4864, 3458) = 2 \cdot 19$.

Lliçó 10

Aritmètica modular

Fixem un enter positiu $N > 1$. Direm que dos enters $a, b \in \mathbb{Z}$ són *congruents mòdul* N, i ho indicarem per $a \equiv b \pmod{N}$, si $N \mid a-b$. Equivalentment, tenim que $a \equiv b \pmod{N}$ si, i només si, els residus a mod N i b mod N coincideixen.

La relació de congruència és d'equivalència, i indicarem per $[a]_N$ ó $[a]$ la classe d'equivalència de a mòdul N,

$$[a] = \{\dots, a-2N, a-N, a, a+N, a+2N, \dots\}.$$

Indicarem per $\mathbb{Z}_N$ el conjunt de classes d'equivalència, i atès que hi ha tantes classes d'equivalència com residus possibles en fer la divisió euclidiana entre N, tenim que

$$\mathbb{Z}_N = \{[0], [1], \dots, [N-1]\},$$

i els enters $0, 1, \dots, N-1$ s'acostumen a fer servir com a representants d'aquestes classes.

Exemple: Prenem $N = 6$; aleshores $\mathbb{Z}_6$ té 6 elements:

$$\begin{aligned}
[0] &= \{\dots, -6, 0, 6, 12, \dots\} \\
[1] &= \{\dots, -5, 1, 7, 13, \dots\} \\
[2] &= \{\dots, -4, 2, 8, 14, \dots\} \\
[3] &= \{\dots, -3, 3, 9, 15, \dots\} \\
[4] &= \{\dots, -2, 4, 10, 16, \dots\} \\
[5] &= \{\dots, -1, 5, 11, 17, \dots\}
\end{aligned}$$

Sobre $\mathbb{Z}_N$ definim operacions de suma i de producte per mitjà de:

$$\begin{aligned}
[a] + [b] &= [a+b] \\
[a] \cdot [b] &= [a \cdot b]
\end{aligned}$$

El fet que aquestes operacions estan ben definides prové del lema següent.

Lema 10: *Suposem que* $a \equiv a' \pmod{N}$ *i* $b \equiv b' \pmod{N}$*; aleshores* $a + b \equiv a' + b' \pmod{N}$ *i* $a \cdot b \equiv a' \cdot b' \pmod{N}$.

PROVA: Siguin k i l tals que $kN = a - a'$ i $lN = b - b'$. Aleshores $(k+l)N = (a+b) - (a'+b')$, d'on $N \mid (a+b) - (a'+b')$ i per tant, $a + b \equiv a' + b' \pmod{N}$. Anàlogament, de $a = a' + kN$ i $b = b' + lN$ obtenim que $ab = a'b' + N(la' + kb' + klN)$, d'on es segueix que $N \mid ab - a'b'$ i per tant, $ab \equiv a'b' \pmod{N}$. □

Exemple: La taula de la suma i el producte a $\mathbb{Z}_6$ és:

+	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[1]	[2]	[3]	[4]	[5]
[1]	[1]	[2]	[3]	[4]	[5]	[0]
[2]	[2]	[3]	[4]	[5]	[0]	[1]
[3]	[3]	[4]	[5]	[0]	[1]	[2]
[4]	[4]	[5]	[0]	[1]	[2]	[3]
[5]	[5]	[0]	[1]	[2]	[3]	[4]

·	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]
[2]	[0]	[2]	[4]	[0]	[2]	[4]
[3]	[0]	[3]	[0]	[3]	[0]	[3]
[4]	[0]	[4]	[2]	[0]	[4]	[2]
[5]	[0]	[5]	[4]	[3]	[2]	[1]

El conjunt $\mathbb{Z}_N$ amb les operacions definides és també un anell:

- $(\mathbb{Z}_N, +)$ és un grup abelià, on l'element neutre és [0], i l'element oposat a un $[a]$ és $[-a]$.
- $(\mathbb{Z}_N, \cdot)$ compleix la propietat associativa i té element neutre, [1].
- $(\mathbb{Z}_N, +, \cdot)$ compleix la propietat distributiva del producte respecte de la suma.

Un $[a] \in \mathbb{Z}_N$ es diu que és *invertible* si existeix un altre $[b] \in \mathbb{Z}_N$ amb $[a] \cdot [b] = [1]$. Els elements invertibles de $\mathbb{Z}_N$ s'indiquen per $\mathbb{Z}_N^*$.

Proposició 11: *Un element* $[a] \in \mathbb{Z}_N$ *és invertible si, i només si,* $\mathrm{mcd}(a, N) = 1$.

PROVA: Suposem que existeix un tal $[b]$ amb $[a] \cdot [b] = [1]$, és a dir, $[ab] = [1]$. D'aquí es segueix que $N \mid 1 - ab$ i, per tant, existeix un k amb $1 = kN + ab$. D'aquí s'obté que $\mathrm{mcd}(a, N) = 1$ per la identitat de Bezout.

Recíprocament, si $\mathrm{mcd}(a, N) = 1$, de la identitat de Bezout se'n dedueix l'existència de $r, s \in \mathbb{Z}$ amb $1 = ra + sN$, d'on tenim que $1 \equiv ra \pmod{N}$ i finalment $[1] = [r] \cdot [a]$. □

Exemple: Els invertibles a $\mathbb{Z}_6$ són $\mathbb{Z}_6^* = \{[1], [5]\}$.

Observem que fent servir l'algorisme estès d'Euclides, podem decidir quan un element $[a] \in \mathbb{Z}_N$ té invers i, en tal cas, trobar-lo explícitament.

Exemple: Fent servir l'algorisme estès d'Euclides, es té que

$$\mathrm{mcd}(2452, 35) = 1, \qquad 1 = (-17) \cdot 2452 + 1191 \cdot 35,$$

d'on tenim que $1 \equiv 1191 \cdot 35 \pmod{2452}$. Per tant, l'invers de $[35]_{2452}$ és $[1191]_{2452}$.

Corol·lari 12: *Sigui p un nombre primer. Tot element $[a] \in \mathbb{Z}_p$ diferent de $[0]$ té invers.*

El nombre d'elements de $\mathbb{Z}_N$ que són invertibles s'indica per $\phi(N)$, anomenada la ϕ d'Euler, i es pot descriure pel nombre d'enters positius menors que N que són relativament primers amb N.

Lema 13: *Siguin $\mathbb{Z}_N^* = \{[x_1], \ldots, [x_k]\}$ els elements invertibles de $\mathbb{Z}_N$ i $[y]$ un invertible qualsevol. Aleshores $\{[y][x_1], \ldots, [y][x_k]\} = \mathbb{Z}_N^*$.*

PROVA: Per a cada $[x_i]$, tenim que $[y][x_i]$ és igual a $[x_{\sigma(i)}]$ per a certa permutació σ dels índexos. En efecte, $[y][x_i]$ té invers $[x_i]^{-1}[y]^{-1}$ i és doncs igual a algun element del conjunt $\{[x_1], \ldots, [x_k]\}$. A més, si $\sigma(i) = \sigma(j)$, tenim que $[y][x_i] = [y][x_j]$ i, per tant, $[x_i] = [x_j]$. □

Teorema 14 (Teorema d'Euler): *Sigui y un enter relativament primer amb N. Aleshores $y^{\phi(N)} \equiv 1 \pmod{N}$.*

PROVA: En termes d'aritmètica modular, hem de provar que si $[y]$ un invertible de $\mathbb{Z}_N$, aleshores $[y]^{\phi(N)} = [1]$. Siguin $[x_1], \ldots, [x_k]$ els elements invertibles de $\mathbb{Z}_N$, on $k = \phi(N)$, i diguem u el producte de tots ells, $u = [x_1] \cdots [x_k]$. Aleshores, pel lema anterior tenim que

$$u = [x_1] \cdots [x_k] = ([y][x_1]) \cdots ([y][x_k]) = [y]^k u,$$

i atès que u és invertible, tenim que $[y]^k = [1]$. □

Corol·lari 15 (Teorema petit de Fermat): *Si p és un nombre primer, aleshores $n^p \equiv n \pmod{p}$ per a tot enter n.*

PROVA: Si $p \mid n$, tenim que $n \equiv 0 \pmod{p}$ i la identitat es compleix de forma trivial. Altrament, $\mathrm{mcd}(p, n) = 1$ i, per tant, n és invertible mòdul p; aleshores $[n]^{\phi(p)} = [n]^{p-1} = [1]$, d'on es segueix que $[n]^p = [n]$ i, per tant, $n^p \equiv n \pmod{p}$. □

Lliçó 11

Teorema xinès dels residus

Considerem la congruència

$$x \equiv a \pmod{M},$$

i pensem-la com una equació a solucionar, on les dades són a i M, i x la incògnita. En aquest cas, sempre hi ha infinites solucions:

$$x = \ldots, a-2M, a-M, a, a+M, a+2M, \ldots$$

El teorema xinès dels residus generalitza aquest resultat per a sistemes de congruències.

Teorema 16 (Xinès dels residus): *El sistema*

$$\begin{aligned} x &\equiv a \pmod{M} \\ x &\equiv b \pmod{N} \end{aligned}$$

té solució si, i només si,

$$\mathrm{mcd}(M,N) \mid b-a.$$

En tal cas, i donada una solució x_0, totes les solucions del sistema són les de la congruència

$$x \equiv x_0 \pmod{\mathrm{mcm}(M,N)}.$$

Prova: Suposem que existeix una solució al sistema. Aleshores existeixen enters y i z tals que $x = a + My = b + Nz$. És a dir, amb $My - Nz = b - a$; ara bé, per la identitat de Bezout, això implica que $b - a$ és un múltiple de $\mathrm{mcd}(M, N)$.

Recíprocament, suposem que $\mathrm{mcd}(M, N) \mid b-a$, i siguin y, z enters tals que $My - Nz = b - a$; prenent $x = a + My = b + Nz$ obtenim una solució comú a les dues congruències.

Suposem ara que x_0, x_1 són dues solucions al sistema d'equacions. Aleshores es té que $x_1 - x_0$ és una solució al sistema

$$\begin{aligned} x &\equiv 0 \pmod{M} \\ x &\equiv 0 \pmod{N} \end{aligned}$$

i, per tant, $x_1 - x_0$ és una solució a l'equació

$$x \equiv 0 \pmod{\mathrm{mcm}(M,N)},$$

d'on s'obté el resultat. □

Exemple: Considerem el sistema:

$$\begin{aligned} x &\equiv 11 \pmod{74} \\ x &\equiv 13 \pmod{63} \end{aligned}$$

Les solucions compleixen que existeixen y, z amb

$$x = 11 + 74y = 13 + 63z,$$

d'on tenim que

$$74y - 63z = 2.$$

Fent servir l'algorisme estès d'Euclides obtenim la solució

$$74 \cdot (-17) + 63 \cdot 20 = 2$$

i, per tant, podem prendre $y = -17$ i $z = -20$. Aleshores

$$x = 13 - 63 \cdot 20 = -1247$$

és una solució.

Corol·lari 17 (Teorema xinès dels residus (forma clàssica)): *Siguin M, N nombres positius relativament primers. Aleshores el sistema de congruències*

$$\begin{aligned} x &\equiv a \pmod{M} \\ x &\equiv b \pmod{N} \end{aligned}$$

té sempre solució.

El teorema xinès en aquesta forma clàssica admet una generalització a un nombre arbitrari d'equacions.

Teorema 18: *Siguin $M_1, \ldots, M_k$ nombres positius relativament primers dos a dos. Aleshores el sistema de congruències*

$$x \equiv a_i \pmod{M_i} \qquad (i = 1, \ldots, k)$$

té sempre solució.

Una aplicació interessant del teorema xinès dels residus és una expressió per al càlcul de la funció ϕ d'Euler.

Proposició 19: *1. Siguin m, n enters positius relativament primers. Aleshores*

$$\phi(m \cdot n) = \phi(m)\phi(n).$$

2. *Sigui p un nombre primer i $r \geqslant 1$ un enter. Aleshores*

$$\phi(p^r) = p^r - p^{r-1} = p^{r-1}(p-1) = p^r\left(1 - \frac{1}{p}\right).$$

3. *Si $n = \prod_{i=1}^{k} p_i^{r_i}$ és la descomposició de n en producte de potències de primers diferents,*

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

PROVA: 1. Considerem l'aplicació

$$\begin{aligned} \mathbb{Z}_{mn} &\to \mathbb{Z}_m \times \mathbb{Z}_n \\ [a]_{mn} &\mapsto ([a]_m, [a]_n) \end{aligned}$$

El teorema xinès dels residus implica que un element a és invertible mòdul mn si, i només si, ho és mòdul m i mòdul n. En particular es té que l'aplicació anterior estableix una bijecció entre $\mathbb{Z}_{mn}^*$ i $\mathbb{Z}_m^* \times \mathbb{Z}_n^*$. Per tant, els cardinals d'aquests conjunts coincideixen, d'on s'obté que $\phi(mn) = \phi(n)\phi(m)$.

2. Els nombres a l'interval $0, \ldots, p^r - 1$ que no són relativament primers amb p^r són exactament els múltiples de p (incloent el zero) i, per tant, n'hi ha $p^r/p = p^{r-1}$ d'aquests. El resultat s'obté traient del total dels p^r enters els p^{r-1} enters no relativament primers amb p^r. Les altres expressions s'obtenen de manera immediata.

3. El resultat s'obté fent servir els apartats anteriors. □

Lliçó 12

Aplicacions a criptografia

L'objectiu de la *criptografia* és modificar missatges a enviar per un determinat canal per tal que només puguin ser llegits pel destinatari del missatge.

12.1 Codificació

Habitualment, els missatges són cadenes de text, i el primer procés a fer és *codificar-los*, és a dir, convertir-los en una successió de nombres que podrem tractar. La forma més habitual de codificació és considerar la cadena a tractar, dividir-la en blocs d'una determinada longitud, i cada bloc d'aquests convertir-lo a un nombre. Atès que el nombre de cadenes de longitud fixada sobre un determinat alfabet és finit i fàcilment enumerable, qualsevol enumeració ens dóna una possible codificació del bloc.

Per exemple, els sistemes més senzills prenen blocs de 1 caracter, i aquests es suposa que pertanyen a l'alfabet `A`...`Z`. Aquests caracters es poden codificar fent servir l'ordre de l'alfabet: `A` es codifica per 0, `B` per 1, i així successivament fins `Z` que es codifica per 25. En sistemes més complexos, cada caracter es codifica pel seu codi ASCII (que pren valors de 0 a 127, és a dir, empra 7 bits) o UNICODE (que empra 16 bits).

Per a codificacions que empren blocs amb més d'un caracter, es codifica cadascun dels caracters del bloc i aquests es combinen de manera anàloga a les representacions digitals d'enters. És a dir, si la seqüència de codis dels caracters és $(c_1, \ldots, c_k)$, i cadascun d'aquests està entre 0 i $d-1$, es codifica el bloc per

$$c_1 d^{k-1} + \cdots + c_{k-1} d + c_k.$$

Exemple: Considerem el missatge `Criptografia`. Fem servir blocs de longitud 4 i codifiquem els caracters pel seu codi ASCII. El primer bloc a tractar és `Crip` i els codis ASCII dels seus caracters són $(67, 114, 105, 112)$, com que el codi ASCII codifica amb 128 valors diferents, la codificació d'aquest bloc és:

$$67 \cdot 128^3 + 114 \cdot 128^2 + 105 \cdot 128 + 112 = 142\,390\,512.$$

Procedint de manera anàloga amb els altres blocs, trobem la seqüencia de codis que hauria de ser tractada:

$$142\,390\,512, 245\,101\,554, 205\,108\,449.$$

12.2 Criptografia

Una vegada els missatges han estat codificats, podem pensar en que l'objecte a enviar és un enter m (el missatge), i el que volem és canviar aquest enter m per un altre enter c (el criptograma) de manera que el destinatari pot recuperar m a partir de c, però que qualsevol altre persona que pugui capturar c no pugui recuperar m.

Així, podem descriure matemàticament el procés com un parell de funcions:

$$E : \mathcal{M} \to \mathcal{C}, \qquad D : \mathcal{C} \to \mathcal{M},$$

que passen del conjunt de missatges al conjunt de criptogrames i viceversa. Per tal que tingui sentit, cal que $D(E(m)) = m$ per a tot missatge m.

Habitualment, aquests dos processos depenen d'una *clau* k, i per tant, es descriuen el processos per funcions que depenen d'aquesta clau k, E_k i D_k.

12.3 Xifrat de César

Aquest mètode de xifrat (que feia servir César) empra blocs de 1 caracter, sobre l'alfabet `A...Z`. Per tant, podem considerar el conjunt de missatges $\mathcal{M} = \mathbb{Z}_{26}$. Les funcions d'encriptació i desencriptació són, respectivament:

$$E(x) = x + 3, \qquad D(x) = x - 3,$$

en el benentès que les operacions es realitzen a l'anell $\mathbb{Z}_{26}$.

Exemple: El missatge `ATAQUEU` seria encriptat per `DWDTXHX`.

Altres variants d'aquest xifrat són els xifrats afins, que depenen de paràmetres a i b:

$$E_{a,b}(x) = ax + b, \qquad D_{a,b}(x) = a^{-1}(x - b),$$

on a ha de ser invertible mòdul 26.

12.4 Xifrat RSA

El xifrat RSA és un tipus de xifrat *de clau pública*. Aquests sistemes es caractaritzen perque cada usuari té un parell de claus, la seva *clau pública* k_p (que qualsevol altre usuari pot conèixer) i la seva *clau privada* k_s (que manté en secret). El procés d'encriptació fa servir la clau pública per generar el criptograma a enviar (i per tant, qualsevol usuari pot encriptar un missatge dirigit a un determinat usuari), mentre que el procés de desencriptació fa servir la clau privada (i per tant, només l'usuari a qui va dirigit el missatge el pot desencriptar).

En el sistema de RSA, cada usuari genera la següent informació:

- Dos primers p i q "prou grans" i diferents.
- Es calcula $n = p \cdot q$.
- Es calcula $\phi(n) = (p - 1)(q - 1)$.

- Es tria un enter e, amb $1 < e < \phi(n)$ i amb $\text{mcd}(e, \phi(n)) = 1$.
- Es calcula d invers de e mòdul $\phi(n)$.

Aleshores, la clau pública de l'usuari és el parell

$$k_p = (n, e)$$

i la clau privada el parell

$$k_s = (n, d).$$

El procés d'encriptació és

$$E_{k_p}(m) = m^e \bmod n$$

i el procés de desencriptació

$$D_{k_s}(c) = c^d \bmod n.$$

Observem que, pel teorema d'Euler, la desencriptació d'un criptograma produeix el missatge original. Per poder aplicar aquest sistema s'ha de tenir en compte que els missatges i criptogrames es treballen mòdul n i, per tant, s'han de triar els primers p i q de manera que cada bloc a codificar vingui donat per un enter entre 0 i $n - 1$.

Exemple: Seguim amb l'exemple anterior. Els missatges a codificar tenen $4 \cdot 7 = 28$ bits, de manera que s'han d'escollir primers p i q de forma que $p \cdot q > 2^{28}$:

- Prenem $p = 16\,381$ i $q = 17\,011$.
- Calculem $n = pq = 278\,657\,191$.
- Calculem $\phi(n) = (p-1)(q-1) = 278\,623\,800$.
- Triem l'exponent $e = 155\,327$, que és relativament primer amb $\phi(n)$.
- Calculem l'invers de e mòdul $\phi(n)$, $d = 233\,323\,463$.

Les claus pública i privada són:

$$k_p = (278\,657\,191, 155\,327), \qquad k_s = (278\,657\,191, 233\,323\,463).$$

El primer missatge a xifrar és $m = 142\,390\,512$, que dóna el criptograma

$$c = m^e \bmod n = (142\,390\,512)^{155\,327} \bmod 278\,657\,191 = 229\,531\,282.$$

Aquest criptograma es pot desxifrar per obtenir

$$m = c^d \bmod n = (229\,531\,282)^{233\,323\,463} \bmod 278\,657\,191 = 142\,390\,512,$$

és a dir, el missatge original.

La seguretat d'aquest tipus de sistemes es basa en que, donada la clau pública k_p, és "molt difícil" trobar la clau privada. En el cas del RSA, per tal de, donada k_p, trobar k_s, cal trobar inversos mòdul $\phi(n)$, però donat n, per trobar $\phi(n)$ cal factoritzar l'enter n, i aquest problema és "molt difícil".

Tema 4

Combinatòria

Lliçó 13

Principis combinatoris

L'objectiu principal de la combinatòria (enumerativa) és comptar el nombre d'objectes amb certes propietats. Sovint aquests objectes a comptar s'especifiquen en termes de subconjunts o llistes d'elements de conjunts; altres vegades s'expressen en termes de processos d'elecció.

Els principis combinatoris que exposem a continuació marquen les tècniques a més baix nivell que es poden fer servir per a aquest recompte, i tradueixen al llenguatge combinatori fets provinents de la teoria de conjunts.

13.1 Principi de la bijecció

Tot i que pot semblar una evidència, o fins i tot és la definició mateixa de cardinal, tenim el següent principi:

Principi (de la bijecció): *Si existeix una bijecció entre dos conjunts diferents, aquests tenen el mateix cardinal.*

Així, gairebé mai estem comptant els objectes directament, sinó a través de bijeccions amb altres objectes.

Exemple: En la competició de futbol de la galàxia d'Andròmeda hi participen 1500 equips. Les regles estableixen que tot partit ha de tenir guanyador (no s'admeten empats) i que l'equip que perd un partit és immediatament exclòs de la competició. Es demana quants partits s'hauran de jugar fins conèixer el campió. Observem que cada partit té un equip perdedor, i que un equip perdedor ho és d'un únic partit (ja que quan perd, queda eliminat). Així, es té una bijecció entre el conjunt de partits jugats i el conjunt d'equips perdedors, que té cardinal $1500 - 1 = 1499$. Per tant, es juguen 1499 partits.

13.2 Principis de la suma, el producte i el quocient

Principi (de la suma): *Quan hi ha m casos diferents, de tal forma que per al cas i-èssim hi ha n_i opcions, i cap parell de casos té cap opció en comú, aleshores el nombre total d'opcions és $n_1 + \cdots + n_m$.*

El principi de la suma es pot expressar com: El cardinal de la unió disjunta és igual la suma dels cardinals dels conjunts. És a dir, si $A_1, \ldots, A_m$ són conjunts disjunts dos a dos,

$$|A_1 \sqcup A_2 \sqcup \cdots \sqcup A_m| = |A_1| + |A_2| + \cdots + |A_m|.$$

Exemple: S'ha d'escollir un representant a la junta del Departament. Els elegibles són 25 professors titulars i 6 catedràtics. Hi ha, doncs, 31 eleccions possibles.

Principi (del producte): *Si una tasca es pot descomposar en m passos, de manera que hi ha n_1 opcions per al primer pas, i que una vegada s'ha completat el pas i-èssim, hi ha n_{i+1} opcions per al pas següent, el nombre total de maneres de realitzar la tasca és $n_1 \cdots n_m$.*

El principi del producte es pot expressar com: El cardinal del producte cartesià és igual al producte dels cardinals dels conjunts. És a dir,

$$|A_1 \times A_2 \times \cdots \times A_m| = |A_1| \cdot |A_2| \cdots |A_m|.$$

Exemple: En un determinat llenguatge de programació, les variables s'identifiquen amb cadenes formades per 3 lletres de l'alfabet i 2 dígits decimals. El nombre de possibles noms de variables en aquest llenguatge és $26 \cdot 26 \cdot 26 \cdot 10 \cdot 10 = 1.757.600$.

Principi (del quocient): *Si un conjunt de n objectes s'agrupa en classes, de manera que cada classe conté m objectes, el nombre de classes que hi ha és $\frac{n}{m}$.*

Una formulació alternativa d'aquest principi és que si en un conjunt A amb n elements hi ha definida una relació d'equivalència $\sim$, de manera que cada element té m elements relacionats amb ell, aleshores $|S/\!\sim| = n/m$.

Exemple: En una reunió, hi ha 5 persones que han d'asseure en una taula rodona. Les formes de reordenar aquestes persones és (veure tema següent) $5 \cdot 4 \cdot 3 \cdot 2 = 120$; ara bé, podem agrupar aquestes reordenacions, ja que en asseure's nomes volem tenir en compte les posicions relatives, en classes, i cada classe té 5 elements. Per tant, les formes d'asseure's essencialment diferents és $120/5 = 24$.

Aplicacions

Recompte de funcions. Siguin $A = \{a_1, \ldots, a_m\}$ i $B = \{b_1, \ldots, b_n\}$ conjunts finits, de cardinals respectius m i n.

- Hi ha n^m funcions diferents $A \to B$. En efecte, per tal de determinar una tal funció, hem d'assignar una imatge per a a_1 d'entre les n possibles; una imatge per a a_2 de les n possibles, i així successivament per als m elements de A. El principi del producte proporciona el resultat desitjat.

- Hi ha $n \cdot (n-1) \cdots (n-m+1) = n!/(n-m)!$ funcions injectives $A \to B$. El procés segueix com en el cas anterior, tenint en compte que en el pas i-èssim, no podem assignar a a_i cap de les imatges escollides per a $a_1, \ldots, a_{i-1}$.

Recompte de subconjunts. Sigui A un conjunt finit de cardinal $|A| = n$, aleshores $|\mathcal{P}(A)| = 2^n$. En efecte, cada subconjunt $B \subseteq A$ queda determinat per la seva funció característica $\chi_B : A \to \{0,1\}$, i donada una funció $f : A \to \{0,1\}$ qualsevol, aquesta determina el subconjunt $f^{-1}(1) \subseteq A$. Per tant, hi ha tants subconjunts com a funcions de A en $\{0,1\}$. Per l'apartat anterior, aquest nombre d'aplicacions és 2^n.

13.3 Principi del colomar

Contràriament als principis anteriors, que s'apliquen a trobar el nombre d'objectes amb certes propietats, el principi del colomar (o de Dirichlet) s'aplica per a deduir l'existència d'algun objecte amb certes propietats.

Principi (del colomar): *Si n objectes s'han de posar en k caixes diferents, on $n > k$, almenys una caixa contindrà més d'un objecte.*

El principi del colomar es pot expressar dient que tota funció $f : A \to B$ amb $|A| > |B|$ és no-injectiva.

Exemple: En una reunió de 8 o més persones, n'hi ha dues que han nascut el mateix dia de la setmana. En efecte, podem pensar que posem les persones en 7 caixes que representen els diferents dies de la setmana. Pel principi del colomar, almenys una caixa conté més d'una persona. Una altra formulació possible seria prendre A el conjunt de persones, B el conjunt de dies de la setmana, i $f : A \to B$ l'aplicació que assigna a cada persona el dia en que va néixer.

Principi (del colomar generalitzat): *Si n objectes s'han de posar en k caixes diferents, aleshores alguna caixa conté almenys $\left\lceil \frac{n}{k} \right\rceil$ objectes.*

Exemple: En una reunió de 25 persones, n'hi ha com a mínim 4 que han nascut el mateix dia de la setmana. En efecte, això es segueix del principi del colomar generalitzat, amb $n = 25$ i $k = 7$, ja que $\lceil 25/7 \rceil = 4$.

Aplicacions

Sigui $f : A \to B$ una funció entre conjunts finits. Es té:

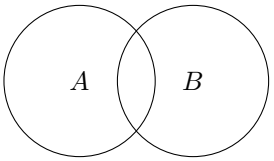
- Si f és injectiva, aleshores $|A| \leqslant |B|$.
- Si f és exhaustiva, aleshores $|A| \geqslant |B|$.
- Si f és bijectiva, aleshores $|A| = |B|$.
- Si f és injectiva i $|A| = |B|$, aleshores f és bijectiva.
- Si f és exhaustiva i $|A| = |B|$, aleshores f és bijectiva.

13.4 Principi d'inclusió/exclusió

El principi de la suma estableix que el cardinal de la unió disjunta de dos conjunts és la suma dels cardinals dels conjunts. En cas que aquests conjunts tinguin intersecció no buida s'ha de descomptar els elements de la intersecció, ja que s'han comptat dues vegades,

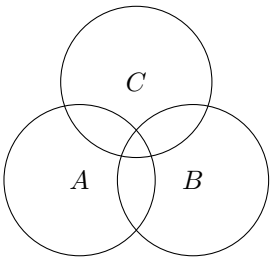
$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Aquesta igualtat es fa evident considerant el diagrama de Venn següent:



Aquesta idea es pot generalitzar a unions de 3 subconjunts,

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



i en general a unions de n subconjunts:

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = \sum_{k=1}^{n} (-1)^{k+1} \sum_{1 \leqslant i_1 < \ldots i_k \leqslant n} |A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k}|$$

Exemple: De 70 persones observades, n'hi ha 37 que beuen cafè, 23 que beuen te, i 25 que no beuen ni te ni cafè. Cal trobar el nombre de persones que beuen te i cafè. Diguem Ω l'univers d'aplicació, el conjunt de persones observades, C el conjunt de persones que beuen cafè, i T el conjunt de persones que beuen te. Com que $|\overline{C \cup T}| = 25$, tenim que $|C \cup T| = 70 - 25 = 45$ i de la fórmula del principi d'inclusió/exclusió, tenim: $45 = 37 + 23 - |C \cap T|$, d'on $|C \cap T| = 15$.

Lliçó 14

Permutacions i combinacions

14.1 Permutacions (sense repetició)

Considerem un conjunt S de n elements. Una *permutació* de S és una bijecció de S en ell mateix. Alternativament, podem definir una permutació com una ordenació (o llista ordenada sense repetició) $(a_1, \ldots, a_n)$ dels elements de S; amb aquesta aproximació, una permutació és una bijecció de $[n]$ en S, de manera que la imatge d'un cert $i \in [n]$ és l'element que ocupa la posició i-èssima en aquesta ordenació.

Fent servir els resultats d'enumeració de funcions injectives, aquest nombre de permutacions és

$$P(n) = n!.$$

Sovint és interessant en lloc d'obtenir llistes ordenades de tots els elements d'un conjunt, obtenir llistes amb menys elements. Així, una k-permutació d'un conjunt S amb n elements és una llista ordenada de k elements escollits d'entre els de S. Observem que donar una tal k-permutació equival a donar una aplicació $[k] \to S$ injectiva.

Fen servir el mateix argument que en el cas anterior, obtenim que hi ha $n \cdot (n-1) \cdots (n-k+1) = n!/(n-k)!$ maneres d'obtenir k-permutacions d'un conjunt de n elements, cosa que indiquem per

$$P(n,k) = \frac{n!}{(n-k)!}.$$

Exemple: Es té una baralla de 52 cartes. El nombre de maneres diferents d'ordenar-les és 52!, és a dir,

806581751709438785716606368564037669752895054408832778240000000000,

un nombre amb 68 dígits. El nombre de maneres de treure'n 5 cartes ordenades és 52!/47!, és a dir,

311.875.200.

Exemple: Es tenen k boles de colors diferents, que s'han de posar dins de n (amb $n \geqslant k$) caixes diferents, de manera que cada caixa contingui com a màxim una bola. Aquesta assignació es pot fer de $P(n,k)$ maneres diferents. En efecte, es pot pensar aquesta assignació com una funció del conjunt de boles al conjunt de caixes, i aquesta ha de ser injectiva.

14.2 Combinacions (sense repetició)

Considerem un conjunt S de n elements. Una k-combinació de S és un subconjunt de S amb k elements. Alternativament, podem veure una k-combinació com una llista de k elements diferents de S on l'ordre no és rellevant.

Sobre el conjunt de k-permutacions de S, es defineix la relació

$$(a_1,\dots,a_k) \sim (b_1,\dots,b_k) \iff \{a_1,\dots,a_k\} = \{b_1,\dots,b_k\},$$

es a dir, es fan equivalents les k-permutacions que contenen els mateixos elements sense importar l'ordre. Aquesta relació és clarament d'equivalència, i les seves classes d'equivalència es corresponen amb les k-combinacions de S. Atès que la classe d'equivalència de cada k-permutació en conté $k!$, tenim pel principi del quocient que el nombre de k-combinacions és

$$C(n,k) = \frac{n!}{k!(n-k)!} = \binom{n}{k}$$

Exemple: Es té una baralla de 52 cartes. El nombre de mans possibles de 5 cartes és $\binom{52}{5}$ és a dir,

2.598.960.

Exemple: Es tenen k boles iguals, que s'han de posar dins de n (amb $n \geqslant k$) caixes diferents, de manera que cada caixa contingui com a màxim una bola. Aquesta assignació es pot fer de $C(n,k)$ maneres diferents. En efecte, es pot pensar aquesta assignació com escollir un subconjunt de k caixes d'entre les n possibles; les escollides seran les que contindran boles, i les restants quedaran buides.

14.3 Identitats binomials

Els nombres $\binom{n}{k}$ s'anomenen *coeficients binomials* o *nombres combinatoris*, i compleixen moltes propietats. Algunes d'aquestes són:

- Simetria:
$$\binom{n}{k} = \binom{n}{n-k.}$$
En efecte, hi ha tantes maneres d'escollir k elements entre n possibles com d'escollir-ne $n-k$; els que ens quedem en un cas són els que rebutgem en l'altre.

- Recursió de Pascal:
$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}.$$
Pensem que volem comptar el nombre de k-subconjunts d'un conjunt de n elements. Podem partir aquests k-subconjunts entre aquells que contenen l'element n-èssim i aquells que no el contenen. Dels primers, n'hi ha tants com $(k-1)$-subconjunts d'un conjunt amb $n-1$ elements, mentre que dels segons, n'hi ha tants com a k-subconjunts d'un conjunt amb $n-1$ elements.

- Suma de binomials:
$$\sum_{i=0}^{n} \binom{n}{i} = \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n-1} + \binom{n}{n} = 2^n.$$
En efecte, el terme de l'esquerra compta el nombre de subconjunts amb $0, 1, \ldots, n-1, n$ elements, és a dir, tots els subconjunts possibles, que són 2^n.

- Fórmula del binomi de Newton:
$$(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}.$$
En desenvolupar la potència, surten productes amb les variables x i y. Cada sumand contribueix en una unitat a un monomi de la forma $x^i y^{n-i}$ exactament quan s'escull i vegades x i $n-i$ vegades y.

  Aquesta fórmula pot ser emprada per a demostrar moltes identitats sobre nombre combinatoris. Per exemple, prenent $x = -1, y = 1$ obtenim que
$$\sum_{i=0}^{n} (-1)^i \binom{n}{i} = \binom{n}{0} - \binom{n}{1} + \cdots + (-1)^{n-1} \binom{n}{n-1} + (-1)^n \binom{n}{n} = 0.$$

14.4 Permutacions i combinacions amb repetició

En tractar les permutacions ordinàries (sense repetició), hem vist que es poden modelar per aplicacions injectives $[k] \to S$, amb la imatge d'un determinat enter i, corresponent a l'element que ocupa la posició i-èssima.

Si estem interessats en permutacions que permetin que un determinat element aparegui tants cops com volguem, això ve modelat per aplicacions no necessàriament injectives $[k] \to S$. Com s'ha vist en l'apartat de recompte de funcions, hi ha
$$PR(n,k) = n^k$$
possibilitats diferents.

Una altra variant d'aquestes permutacions amb repetició consisteix en imposar el nombre exacte de cops que cada element pot aparèixer. Suposem donat un conjunt $S = \{s_1, \ldots, s_n\}$ i volem trobar les llistes ordenades de longitud k que podem crear a partir de S, de manera que cada element s_i aparegui exactament k_i vegades; evidentment, tenim $k = k_1 + \cdots + k_n$. Com a objecte intermedi, considerem el conjunt S^*,
$$S^* = \{(s_i, j) \mid s_i \in S, j \in \{1, \ldots, k_i\}\},$$
és a dir, cada s_i apareix tantes vegades com la multiplicitat k_i, i les diferents còpies venen indexades per la segona component. Aleshores $|S^*| = k$ i, per tant, hi ha $k!$ reordenacions possibles. Ara,

agrupem aquestes reordenacions si només difereixen en les seves segones components; com que hi ha k_i elements amb la primera component igual a s_i (per a $i = 1 \ldots, n$), resulta que cada agrupació conté $k_1! \cdots k_n!$ reordenacions diferents de S^*. Pel principi del quocient, resulta que hi ha

$$PR(n, k; k_1, \ldots, k_n) = \frac{k!}{k_1! \cdots k_n!}$$

permutacions diferents.

Exemple: Es pretén comptar el nombre de cadenes binàries de longitud n amb k 0's i, per tant, $n - k$ 1's. És a dir, volem comptar el nombre de permutacions amb repetició de longitud n amb dos elements diferents, que apareixen, respectivament, k i $n - k$ vegades. Per tant, el nombre d'aquestes permutacions és

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

Pel que respecta a combinacions amb repetició, intuïtivament, s'han d'admetre repeticions d'elements, però sent irrellevant el seu ordre. El model matemàtic més adient és, doncs, el multiconjunt. Donat un conjunt S, de cardinal n, indicarem per $S^{\oplus k}$ el multiconjunt que conté els elements de S, tots ells amb multiplicitat k. Així, una *combinació amb repetició d'ordre k* és un sub-multiconjunt del multiconjunt $S^{\oplus k}$ de cardinal k. Equivalentment, podem veure aquest sub-multiconjunt com una funció

$$f : S \to \mathbb{Z}_{\geqslant 0},$$

on la imatge d'un s indica el número de cops que apareix, de manera que $\sum_{s \in S} f(s) = k$.

Per tal de fer el recompte d'aquestes combinacions amb repetició, considerem que enumerem els elements de S, $s_1, \ldots, s_n$, i cada funció descrita anteriorment la representem per una cadena amb els símbols | i •:

$$\underbrace{\bullet \cdots \bullet}_{f(s_1)} | \underbrace{\bullet \cdots \bullet}_{f(s_2)} | \cdots\cdots | \underbrace{\bullet \cdots \bullet}_{f(s_n)}$$

Observem que en aquesta cadena apareix k vegades • i $n - 1$ vegades |. Recíprocament, tota cadena en els símbols $\{\bullet, |\}$ de longitud $n + k - 1$ i amb k vegades • i $n - 1$ vegades | es pot interpretar com a una combinació amb repetició. En efecte, el nombre de cops que apareixerà el primer element serà el nombre de •'s que apareixen abans del primer |; el nombre de cops que apareixerà el segon, serà el nombre de •'s entre el primer i el segon |, i així, successivament. Pel principi de la bijecció tenim que

$$CR(n, k) = \binom{n + k - 1}{k}.$$

Tema 5

Teoria de Grafs

Lliçó 15

Grafs no dirigits

15.1 Grafs

Un *graf no dirigit*, o simplement un *graf*, és un parell $G = (V, E)$ format per un conjunt $V = V(G)$ d'elements que anomenem *vèrtexos* i un conjunt $E = E(G)$ de parells no ordenats de vèrtexos diferents que s'anomenen *arestes*. Sovint s'accepten arestes amb extrems iguals; en tal cas s'anomenen *llaços*.

Un *multigraf* és un graf on s'accepten múltiples arestes unint un mateix parell de vèrtexos. Així, els conjunt d'arestes es substitueix per un multiconjunt d'arestes.

Una aresta $e = \{u, v\}$ es diu que *uneix* els vèrtexos u i v, i en tal cas es diu que u i v són vèrtexos *adjacents*; també es diu que u i v són els *extrems* de e, o que el vèrtex u (o v) i l'aresta e són *incidents*. Per tal de fer les notacions més curtes, s'indica també l'aresta $\{u, v\}$ per uv, en el benentès que uv i vu indiquen la mateixa aresta. Si no hi ha cap aresta unint dos vèrtexos, es diu que aquests són *independents*. Anàlogament, dues arestes es diuen *independents* si no comparteixen cap extrem.

El nombre de vèrtexos d'un graf s'anomena el seu *ordre*, i el nombre d'arestes la seva *mida*.

Els grafs s'acostumen a representar per dibuixos al pla, amb els vèrtexos representats per punts i les arestes per línies que uneixen els seus extrems.

15.2 Graus

Donat un vèrtex u, s'indica per $\Gamma(u)$ el conjunt dels vèrtexos adjacents amb u, i per $d(u)$ el *grau* de u, el nombre dels vèrtexos adjacents a u. Si un graf presenta llaços, cadascun d'aquests contribueixen en 2 unitats al grau del vèrtex.

El *grau màxim* i *grau mínim* d'un graf es defineixen com

$$\delta(G) = \min_{u \in V} d(u), \qquad \Delta(G) = \max_{u \in V} d(u).$$

Un graf on $\delta = \Delta$ compleix que tots els seus vèrtexos tenen igual grau d, i es diu que aquest graf és *d-regular*.

Teorema 20 (Lema de les encaixades de mans): *Tot graf $G = (V, E)$ compleix que*

$$2|E| = \sum_{u \in V} d(u).$$

PROVA: Cada aresta (no llaç) contribueix en una unitat en el grau dels seus dos extrems. Tot llaç contribueix en dues unitats al grau del seu únic extrem. □

Corol·lari 21: *Tot graf té un nombre parell de vèrtexos amb grau senar.*

15.3 Subgrafs

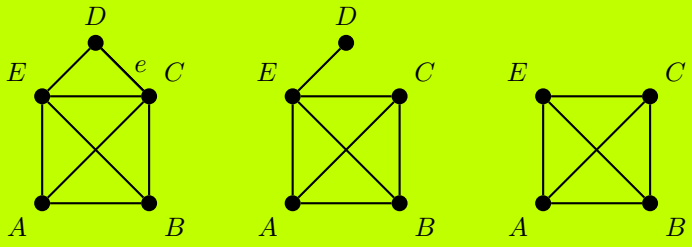
Un graf $G' = (V', E')$ és un *subgraf* de $G = (V, E)$ si $V' \subseteq V$ i $E' \subseteq E'$, és a dir, si s'obté eliminant vèrtexos i arestes de l'original. Quan $V' = V$, és a dir eliminem únicament arestes, es diu que és un *subgraf generador*.

Donat $V' \subseteq V$, el *subgraf induït* per V', que indiquem per $G[V']$, és el subgraf $G' = (V', E')$, amb $E' = E \cap V'^{(2)}$, és a dir, amb les arestes de G que tenen extrems a V'.

Donat $W \subseteq V$, s'indica per $G - W$ el subgraf $G[V \setminus W]$, és a dir, el subgraf que resulta d'eliminar els vèrtexos de W i les arestes incidents amb ells. Si W conté un únic vèrtex w, s'indica $G - w = G - W$.

Donat $F \subset E$, es defineix el subgraf $G - E = (V, E \setminus F)$, és a dir, el resultant d'eliminar les arestes a F, mantenint el mateix conjunt d'arestes. Anàlogament al cas de vèrtexos, si e és una aresta, s'indica per $G - e$ el subgraf $G - \{e\}$.

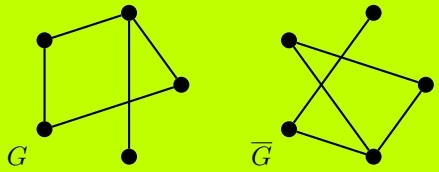
Exemple: En la figura següent es representen els grafs G, $G - e$ i $G - D$.



15.4 Operacions amb grafs

El *complementari* d'un graf $G = (V, E)$ és el graf $\overline{G} = (V, \overline{E})$, és a dir, dos vèrtexos són adjacents a $\overline{G}$ si, i només si, no ho són a G.

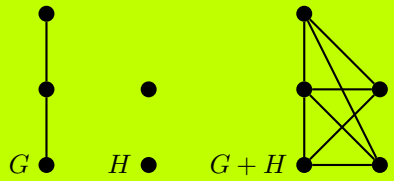
Exemple:



Donats dos grafs G i H, el seu *graf unió* és el graf $G \cup H = (V(G) \cup V(H), E(G) \cup E(H))$. Per exemple, tot graf és la unió dels seus components connexos. Anàlogament, el *graf intersecció* és $G \cap H = (V(G) \cap V(H), E(G) \cap E(H))$.

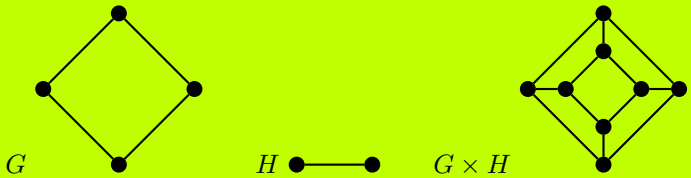
El *graf suma* de dos grafs G i H amb conjunt de vèrtexos disjunts és el graf, indicat per $G+H$, amb vèrtexos $V(G) \cup V(H)$ i amb arestes $E(G) \cup E(H) \cup \{uv \mid u \in V(G), v \in V(H)\}$, és a dir, s'afegeixen a les arestes de G i H una aresta entre cada vèrtex de G i cada vèrtex de H.

Exemple:



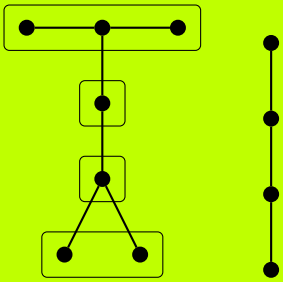
El *graf producte* $G \times H$ és el graf amb vèrtexos $V(G \times H) = V(G) \times V(H)$ i conjunt d'arestes $E(G \times H) = \{(u,v)(u,v') \mid vv' \in E(H)\} \cup \{(u,v)(u'v) \mid uu' \in E(G)\}$.

Exemple:



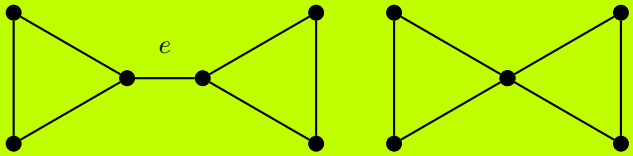
Donat un graf $G = (V, E)$ i una relació d'equivalència $\sim$ sobre els seus vèrtexos, es defineix el *graf quocient* $G/\sim$ que té per vértexos les classes d'equivalència $V/\sim$ i dues classes $[u]$ i $[v]$ són adjacents a $G/\sim$ si, i només si, existeixen representants $u' \sim u$ i $v' \sim v$ amb $u'v' \in E$.

Exemple:



El graf que s'obté per *contracció* d'una aresta $e = uv$ és el graf quocient $G/\sim$, on $\sim$ té per classes d'equivalència $\{u, v\}$ i tots els singletons $\{w\}$ (amb $w \neq u, v$).

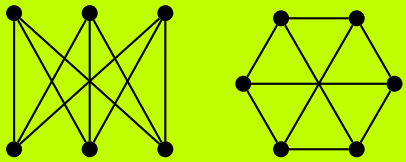
Exemple:



15.5 Isomorfisme

Dos grafs G i H es diuen *isomorfs* si existeix una bijecció entre els seus vèrtexos respectius, $\phi : V(G) \to V(H)$ que respecta l'adjacència, és a dir, que compleix que $\{u, v\} \in E(G)$ si, i només si, $\{\phi(u), \phi(v)\} \in E(H)$. Per al cas de multigrafs s'exigeix, a més, que les corresponents multiplicitats de les arestes coincideixin.

Exemple: Els grafs següents són isomorfs.

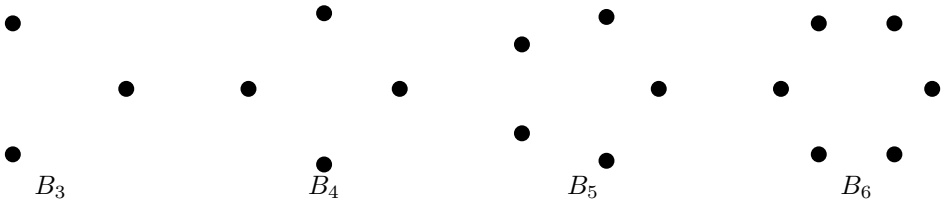


Hi ha certs paràmetres en un graf que són *invariants de la classes d'isomorfisme*, és a dir, no canvien en prendre grafs isomorfs. Per exemple, l'ordre, la mida i la seqüència (no ordenada) dels graus dels seus vèrtexos són invariants. Notem, però, que grafs no isomorfs poden tenir els mateixos invariants.

15.6 Propietats i grafs distingits

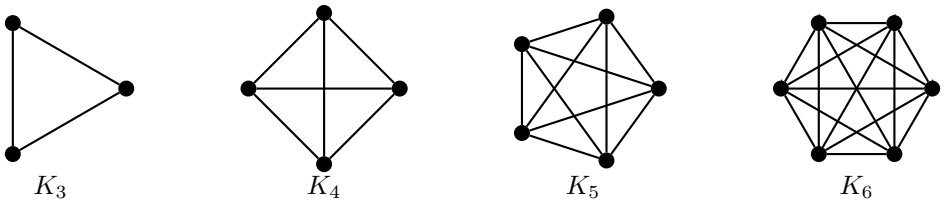
Algunes famílies distingides de grafs són:

- Graf buit B_n: Té n vèrtexos i cap aresta.



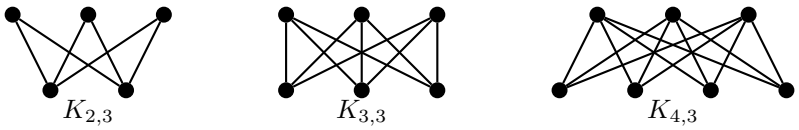
  Es diu que un graf és *buit* si té vèrtexos, però no arestes.

- Graf complet K_n: Té per conjunt de vèrtexos $v_1, \ldots, v_n$ i tot parell de vèrtexos diferents són adjacents. Es pot també descriure com el complementari del graf buit d'ordre n.



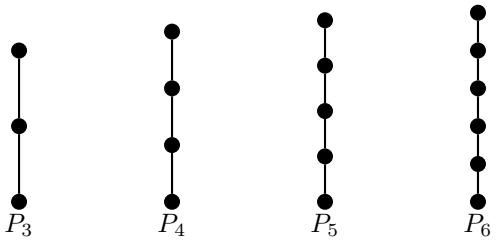
  Un graf es diu *complet* si tot parell de vèrtexos diferents estan units per una aresta.

- Graf bipartit complet $K_{n,m}$: Té per vèrtexos $v_1, \ldots, v_n, u_1, \ldots, u_m$ i arestes tots els $u_i v_j$. Una descripció possible és $B_n + B_m$.

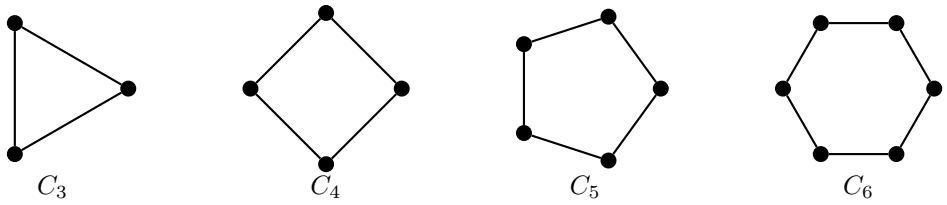


  Un graf es diu *bipartit* si el seu conjunt V de vèrtexos es pot partir en dos subconjunts disjunts V_1, V_2, de manera que tota aresta uneix un vèrtex de V_1 amb un vèrtex de V_2; és a dir, no hi ha cap parell de vèrtexos adjacents dins cadascun dels conjunts que formen la partició.

- Graf camí P_n: Té vèrtexos $v_1, \ldots, v_n$ i arestes que uneixen cada v_i amb v_{i+1} (amb $i = 1, \ldots, n-1$).

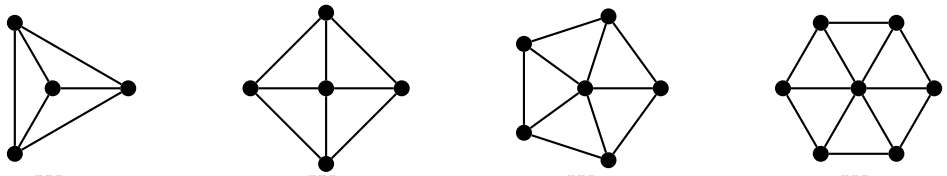


- Graf cicle C_n: S'obté afegint a P_n l'aresta $v_n v_1$.



C_3 C_4 C_5 C_6

- Graf roda W_n: S'obté afegint a C_n un vèrtex v_0 i les arestes de la forma v_0v_i (amb $i = 1, \ldots, n$).



W_3 W_4 W_5 W_6

- Graf hipercub de dimensió n, Q_n: Té per vèrtexos les paraules binàries de longitud n, i dues paraules són adjacents si difereixen en exactament una posició. Es pot descriure per $K_2^n = K_2 \times \cdots \times K_2$.

Lliçó 16

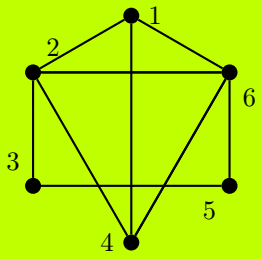
Connectivitat

Un *recorregut* de *longitud* l en un graf G és una seqüència de vèrtexos $(u_0, u_1, \ldots, u_l)$ on, per a tot $i = 1, \ldots, l$ es té que $e_i = u_{i-1}u_i$ són arestes de G. Els vèrtexos $u_0, \ldots, u_l$ s'anomenen els vèrtexos del recorregut, i les arestes e_i les seves arestes. El vèrtex u_0 s'anomena el *vèrtex inicial*, v_l el *vèrtex final*, i els restants els *vèrtexos intermedis*. Es diu també que el recorregut *porta* de u a v.

Un recorregut es diu *simple* si les seves arestes són diferents dues a dues. Un *camí* és un recorregut tal que els seus vèrtexos són tots ells diferents.

Un recorregut es diu que és un *circuit* si el seu vèrtex inicial i final coincideixen, $u_0 = u_l$; en cas de camins, aquests s'anomenen *cicles*, i cal notar que la condició de no repetició dels vèrtexos es compleix llevat de $v_0 = v_l$.

Exemple: Considerem el graf de la figura:



Aleshores:

- $1, 4, 2, 6, 5, 3, 2, 1, 6$ és un recorregut,
- $1, 4, 2, 6, 5, 3$ és un camí,
- $1, 4, 2, 6, 5, 3, 2, 1$ és un circuit,
- $1, 4, 2, 6, 1$ és un cicle.

Es diu que un vèrtex v és *accessible* des d'un altre vèrtex u si existeix un recorregut (eventualment de longitud 0) que té u com a vèrtex inicial i v com a vèrtex final.

Proposició 22: *La relació d'accessibilitat és d'equivalència.*

PROVA:
- Tot vèrtex és accessible des d'ell mateix per un camí de longitud 0.
- Si v és accessible des de u, es té que existeix un recorregut $u = u_0, u_1, \ldots, u_l = v$; aleshores $v = u_l, \ldots, u_1, u_0$ és també un recorregut que porta de v a u.
- Si v és accessible des de u, i w accessible des de v, es tenen recorreguts $u = u_0, u_1, \ldots, u_l = v$ i $v = v_0, v_1, \ldots, v_m = w$; concatenant aquests recorreguts s'obté el recorregut $u = u_0, u_1, \ldots, u_l = v = v_0, v_1, \ldots, v_m = w$ que porta de u a w. □

Observem que podem parlar indistintament de l'existència de recorreguts o de camins entre vèrtexos, com prova la següent proposició.

Proposició 23: *Existeix un recorregut des d'un vèrtex u a un vèrtex v, si, i només si, existeix un camí de u a v.*

PROVA: Tot camí és recorregut i, per tant, una de les implicacions és immediata. Suposem que existeix un recorregut de u a v, $u = u_0, u_1, \ldots, u_l = v$. Si el recorregut visita dos cops un mateix vèrtex, és a dir, $u_i = u_j$ $(i < j)$, podem eliminar els vèrtexos $u_{i+1}, \ldots, u_j$ del recorregut, obtenint un nou recorregut més curt. Iterant aquest procés (que necessàriament ha d'acabar, atès que hi ha un nombre finit de vèrtexos) s'arriba a trobar un camí de u a v. □

Els subgrafs generats per cada classe d'equivalència s'anomenen *components connexos* del graf. Un graf es diu *connex* si té un únic component connex, és a dir, si tot vèrtex del graf és accessible des de qualsevol altre. El fet que un graf sigui connex fita inferiorment el seu nombre d'arestes en funció del seu nombre de vèrtexos.

Proposició 24: *Sigui G un graf connex d'ordre n i mida m. Aleshores $m \geqslant n - 1$.*

PROVA: El resultat és trivial per a grafs amb 1 vèrtex. Suposem el resultat provat per a grafs d'ordre $\leqslant n$ i mida $< m$. Si G conté un cicle, sigui e una aresta d'aquest cicle, i diguem $G' = G - e$; aquest graf és connex, té ordre $n' = n$ i mida $m' = m-1$. Per hipòtesi d'inducció, tenim $m' \geqslant n'-1$, d'on obtenim que $m = m' + 1 \geqslant n' = n > n - 1$ i es té el resultat. Si G' no té cicles, considerem $u = u_0, u_1, \ldots, u_l = v$ un recorregut simple dins G de longitud màxima. El vèrtex v ha de tenir grau 1 (altrament podriem allargar el recorregut per l'aresta incident a v diferent de $u_{l-1}v$). Considerem el graf $G' = G - v$; aquest graf és connex, té ordre $n' = n - 1$ i mida $m' = m - 1$. Per hipòtesi d'inducció, tenim que $m' \geqslant n' - 1$, d'on obtenim que $m \geqslant n - 1$ i es té el resultat. □

En un graf connex, es defineix la *distància* entre dos vèrtexos u i v com la longitud del camí més curt que porta de u a v.

Proposició 25: *La distància definida compleix els axiomes de distància:*

- $d(u, v) \geqslant 0$, *i* $d(u, v) = 0$ *si, i només si,* $u = v$,
- $d(u, v) = d(v, u)$,
- $d(u, w) \leqslant d(u, v) + d(v, w)$ *(desigualtat triangular).*

PROVA: De la definició en resulta inmediatament que $d(u,v) \geqslant 0$ i que $d(u,u) = 0$; ara, si $d(u,v) = 0$, es té un camí de longitud 0 que porta de u a v, d'on $u = v$.

Si un camí de longitud mínima porta de u a v, aleshores prenent-lo en sentit contrari, porta de v a u; d'aixo en segueix que $d(v,u) \leqslant d(u,v)$ i l'altre desigualtat es segueix de manera immediata.

Donats camins de longitud mínima que porten de u a v i de v a w, respectivament, la seva concatenació porta de u a w, i per tant es té que $d(u,w) \leqslant d(u,v) + d(v,w)$. □

Es defineix el *diàmetre* d'un graf com la distància més gran entre parells de vèrtexos,

$$D(G) = \max_{u,v \in V} d(u,v),$$

i la seva *distància mitjana* com

$$\overline{D} = \frac{1}{|V|^2} \sum_{u,v \in G} d(u,v).$$

La *excentricitat* d'un vèrtex és el màxim de les distàncies als altres vèrtexos. El *radi* d'un graf és el mínim de les excentricitats dels seus vèrtexos,

$$r(G) = \min_{u \in V} \big\{ \max_{v \in V} d(u,v) \big\}.$$

El *centre* d'un graf $Z(G)$ és el conjunt de vèrtexos amb excentricitat igual al radi del graf.

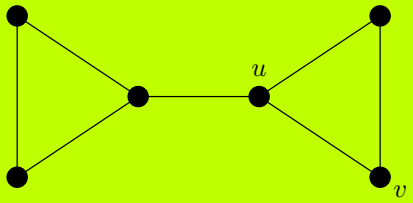
Proposició 26: *Tot graf connex G compleix que*

$$r(G) \leqslant D(G) \leqslant 2r(G).$$

PROVA: La primera desigualtat és immediata a partir de les definicions. Per a la segona, siguin $u, v \in V$ tals que $d(u,v) = D(G)$, i $w \in Z(G)$; aleshores $D(G) = d(u,v) \leqslant d(u,w) + d(w,v) \leqslant 2r(G)$. □

Es diu que un vértex $u \in V(G)$ és un *vértex de tall* si el nombre de components connexos de $G - u$ és major que el de G, és a dir, si en treure aquest vèrtex, el seu component connex esdevé inconnexa.

Exemple: Considerem el graf de la figura:



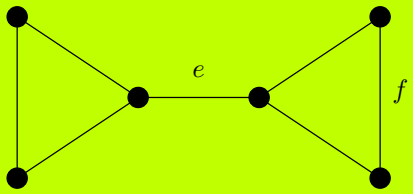
Aleshores u és un vèrtex de tall, mentre que v no ho és.

Proposició 27: *Tot graf connex amb almenys dos vèrtexos té almenys dos vèrtexos que no són de tall.*

PROVA: Suposem que és fals, i sigui G un graf connex on tots els seus vèrtexos són de tall excepte, com a màxim, un. Siguin u, v vèrtexos de G amb $d(u,v) = D(G)$, i podem suposar que v és de tall. Sigui ara w un vèrtex tal que u i w pertanyen a components diferents de $G - v$. Com que tots els camins entre u i w passen per v, tenim que $d(u,w) = d(u,v) + d(v,w) > d(u,v)$ contra la hipòtesi que $d(u,v) = D(G)$. □

Anàlogament, es diu que una aresta $e \in E(G)$ és un *pont* si $G - e$ té més components connexos que G.

Exemple: Considerem el graf de la figura:



Aleshores e és una aresta pont, mentre que f no ho és.

Lliçó 17

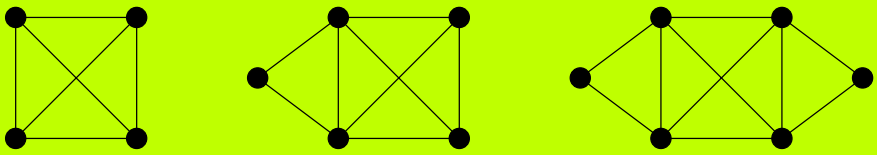
Euler i Hamilton

Un recorregut sobre un graf es diu que és *eulerià* si recorre totes les arestes del graf exactament una vegada. Anàlogament, es diu que un circuit és eulerià si té aquesta mateixa propietat.

Un camí sobre un graf es diu que és *hamiltonià* si recorre tots els vèrtexos del graf exactament una vegada. Anàlogament, es diu que un cicle és hamiltonià si té aquesta mateixa propietat.

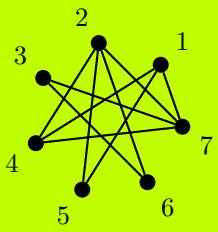
Sovint es diu que un graf és eulerià (resp. hamiltonià) si admet un circuit eulerià (resp. hamiltonià).

Exemple: Considerem els grafs de la figura:



El primer d'ells no admet cap recorregut eulerià; el central admet un recorregut eulerià, però cap circuit eulerià; el tercer admet un circuit eulerià.

Exemple: El graf següent admet un cicle hamiltonià.



El cicle que passa per tots els vèrtexos és :

$$1, 5, 2, 6, 3, 7, 4, 1$$

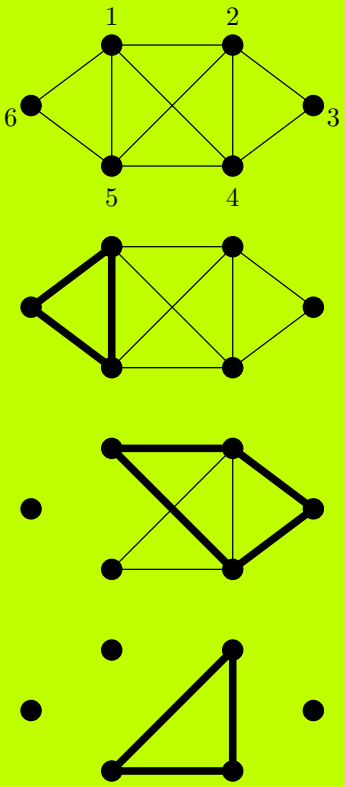
Tot i que les definicions donades indueixen a pensar que la situació és molt semblant en els dos casos, la realitat és que són prou diferents. En particular, donat un graf qualsevol, existeix un algorisme molt senzill per determinar exactament si és, o no, eulerià; en canvi, no es coneix cap criteri senzill per determinar si un graf és hamiltonià o no.

Teorema 28: *Un graf admet un circuit eulerià si, i només si, és connex i tot vèrtex seu té grau parell.*

PROVA: Per a la necesitat, observem que en recórrer un circuit eulerià, cada cop que visitem un vèrtex per una aresta, tornem a sortir d'ell per una altra aresta. Com que mai es visita dos cops una mateixa aresta, tenim que cada vèrtex té un nombre parell d'arestes incidents.

Suposem ara que G és un graf connex amb tots els vèrtexos de grau parell. Construim un recorregut arbitrari partint d'un vèrtex v_0 qualsevol i sense emprar dos cops la mateixa aresta. En arribar a un vèrtex $x \neq v_0$, com que x té grau parell, podem extendre el recorregut a un altre vèrtex. Eventualment, tornem a v_0 i obtenim un circuit C_0. Si C_0 conté totes les arestes de G, hem acabat. Altrament, sigui G' el graf que resulta d'eliminar de G les arestes de C_0, i prenem H un component connex seu amb almenys una aresta. El graf H compleix que és connex i té tots els vèrtexos de grau parell. A més, atès que G és connex, H ha de contenir algun vèrtex v_1 de C_0. Aplicant el mateix procediment anterior, obtenim un circuit C_1 dins H amb orígen i final a v_1. Com que v_1 també forma part de C_0, podem enllaçar aquests dos circuits per obtenir-ne un altre amb més arestas que C_0. Si aquest nou circuit no conté totes les arestes de G, tornem a iniciar el procés. Eventualment, com que G és finit, aquest procés acaba i trobem un circuit eulerià dins G. □

Exemple: La figura següent ilustra aquest procés.



Concatenant els cicles obtinguts, trobem el circuit eulerià: $1, 5, 6, 1, 2, 3, 4, 2, 5, 4, 1$.

Corol·lari 29: *Un graf admet un recorregut eulerià si, i només si, és connex i tot vèrtex seu té grau parell, llevat de com a màxim dos vèrtexos de grau senar.*

PROVA: La necessitat es segueix de manera anàloga al cas anterior, tenint en compte que els vèrtexos inicial i final es visiten un cop més que els intermedis.

Per a la suficiència, donat un tal graf, afegim una aresta entre els dos vèrtexos de grau senar. El graf resultant té tots els vèrtexos de grau parell i, pel resultat anterior, admet un circuit eulerià. Si al circuit eulerià li treiem l'aresta que hem afegit artificialment, obtenim un recorregut que passa per totes les arestes del graf original. □

La situació per a grafs hamiltonians és completament diferent. De fet, no existeix cap manera "senzilla" de decidir si, donat un graf, conté un circuit hamiltonià.

En canvi, es coneixen algunes situacions particulars en les quals es pot determinar la hamiltonicitat d'un graf.

Teorema 30: *Sigui G un graf amb n vèrtexos i m arestes.*

1. *Si $n \geqslant 3$ i tot vèrtex té grau $\geqslant n/2$, aleshores G és hamiltonià.*

2. *Si $n \geqslant 3$ i per a tot parell de vèrtexos no adjacents u i v es compleix que $d(u)+d(v) \geqslant n$, aleshores G és hamiltonià.*
3. *Si $n \geqslant 3$ i $m \geqslant (n^2 - 3n + 6)/2$, aleshores G és hamiltonià.*

També es coneixen conseqüencies del fet que un graf sigui hamiltonià i, per tant, es poden fer servir per decidir que un graf no és hamiltonià.

Teorema 31: *Sigui G un graf hamiltonià. Aleshores:*

1. *G no té vèrtexos de tall.*
2. *Si S és un subconjunt de vèrtexos, el graf $G - S$ té com a molt $|S|$ components connexos.*

Lliçó 18

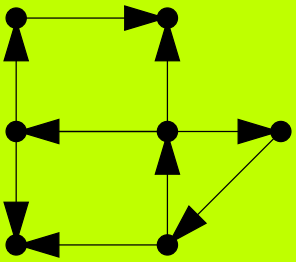
Grafs dirigits

18.1 Digrafs

Un *digraf* o *graf dirigit* és, intuitivament, un graf on a les arestes se'ls hi assigna un sentit. Així, un digraf és un parell $G = (V, A)$ format per un conjunt $V = V(G)$ de vèrtexos i un conjunt $A = A(G)$ de parells ordenats de vèrtexos que anomemen *arcs*. Com en el cas de grafs no dirigits, sovint s'accepten *llaços* i arcs amb multiplicitat.

Els digrafs es representen gràficament com els grafs, indicant l'orientació dels arcs amb una fletxa.

Exemple:



Un arc $e = (u, v)$ es diu que *porta* u a v; en tal cas, es diu que u és un *pare* de v (o que u és *adjacent cap a* v) o que v és un *fill* de u (o que v és *adjacent des de* u). L'arc (u, v) s'indicarà també, per brevetat, com uv.

El conjunt de fills i pares d'un vèrtex $u \in V$ s'indica respectivament per

$$\Gamma_e(u) = \{v \in V \mid vu \in A\},$$
$$\Gamma_s(u) = \{v \in V \mid uv \in A\},$$

i els seus cardinals són el *grau de sortida* i *grau d'entrada*, respectivament, del vèrtex,

$$d_e(u) = |\Gamma_e(u)|, \qquad d_s(u) = |\Gamma_s(u)|.$$

En aquest cas, el lema de les encaixades de mans s'escriu com:

$$|A| = \sum_{u \in V} d_e(u) = \sum_{u \in V} d_s(u).$$

Donat un digraf G, s'anomena el *graf no dirigit subjacent* el graf que s'obté en suprimir l'orientació dels arcs; és a dir, té per vèrtexos els mateixos que G i dos vèrtexos u, v estan units per una aresta si uv o vu és una arc de G.

Les operacions amb digrafs es defineixen i indiquen de la mateixa manera que per grafs no dirigits.

18.2 Connectivitat

En un digraf, els conceptes de recorregut, camí, circuit i cicle s'adapten d'aquests mateixos conceptes per a grafs no dirigits, on ara s'ha de tenir en compte l'orientació. Així, un recorregut és una successió de vèrtexos $v_0, v_1, \ldots, v_l$ on es tenen arcs $v_{i-1}v_i$ $(1 \leqslant i \leqslant l)$.

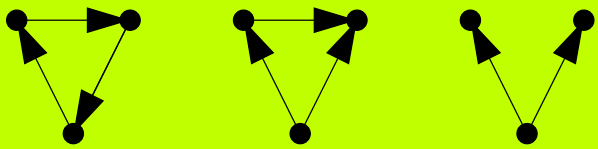
Un vèrtex v es diu que és *accessible* des d'un vèrtex u si existeix un recorregut de u a v; dos vèrtexos u, v es diu que són *mútuament accessibles* si existeixen camins de u a v i de v a u. La relació d'accessibilitat mútua és d'equivalència.

El fet que els camins no siguin reversibles fa que apareguin diferents nocions de connexitat. Així, un digraf es diu que és:

- *dèbilment connex* si el seu graf no dirigit subjancent és connex;
- *unilateralment connex* si per a tot parell de vèrtexos u, v, o bé v és accessible des de u o bé u és accessible des de v.
- *fortament connex* si parell de vèrtexos són mútuament accessibles.

Observem que la connexitat forta implica la unilateral, i aquesta implica la dèbil.

Exemple: Considerem els digrafs de la figura:

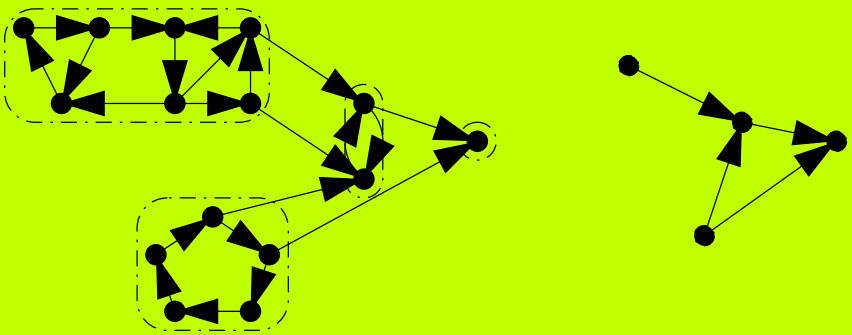


El primer d'ells és fortament connex, el segon és unilateralment connex (però no fortament connex) i el tercer és dèbilment connex (però no unilateralment connex ni fortament connex).

Així mateix, la distància entre vèrtexos deixa de complir els axiomes de distància i, per tant, no es considera.

Donat un digraf, es considera el seu *graf condensat*, que es definiex com el graf quocient respecte de la relació d'accessibilitat mútua.

Exemple: A la figura següent apareix un graf i el seu graf condensat.



18.3 DAGs

Un tipus especial de grafs dirigits son els *grafs dirigits acíclics* o DAGs (de l'anglès *directed acyclic graph*), caracteritzats pel fet que no tenen cicles.

En un DAG, la relació sobre els vèrtexos definida per: $u \succcurlyeq v$ si existeix un camí de u a v és una relació d'ordre parcial. En efecte,

- Tot vèrtex està unit a ell mateix per un camí de longitud zero; d'aquí s'obté que la relació compleix la propietat reflexiva.
- Si existís un camí de u a v i un camí de v a u, concatenant els dos camins s'obtindria un cicle, cosa que és impossible; d'aquí s'obté la propietat antisimètrica.
- Si hi ha camins respectius entre u i v i entre v i w, concatenant-los s'obté un camí de u a w; d'aquí s'obté la propietat transitiva.

Així, tot DAG determina un poset, de la mateixa manera que un poset determina el DAG donat pel seu diagrama de Hasse.

Un vèrtex v d'un digraf es diu que és una *arrel* si no té arcs entrants, és a dir, $d_e(v) = 0$; anàlogament, es diu que és una *fulla* si no té arcs sortints, és a dir, $d_s(v) = 0$. En el llenguatge de posets, les arrels són els elements maximals de $(V, \succcurlyeq)$, mentre que les fulles en són els minimals. Notem que tot DAG té arrels i fulles, atès que es té un poset sobre un conjunt finit.

Proposició 32: *El graf condensat d'un digraf qualsevol és un DAG.*

PROVA: Suposem que existeix un cicle $[u_0], [u_1], [u_2], \ldots, [u_k] = [u_0]$ al graf condensat. Aleshores existeixen representants $v_i, w_i \in [u_i]$ tals que $v_i w_{i+1}$ és un arc de G. El fet que els v_i i w_i pertanyin a la mateixa classe implica l'existència de camins de w_i a v_i; concatenant els arcs i camins trobats, s'arriba a un recorregut $u_0, \ldots, v_0, w_1, \ldots, v_1, w_2, \ldots, v_k, w_k, \ldots, u_0$, cosa que implica que tots els vèrtexos trobats són mútuament accessibles. Per tant, $[u_0] = [u_1] = \cdots = [u_k]$ i el cicle al graf condensat és trivial. □

Lliçó 19

Aspectes computacionals

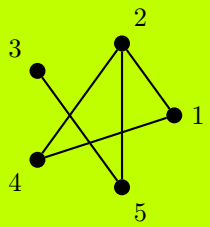
Un dels trets fonamentals dels grafs és que es fan servir en entorns computacionals, on es processen grafs (i digrafs) amb un nombre de vèrtexos i arestes (arcs) que pot ser molt gran. Així, és necessari tenir mètodes per emmagatzemar grafs, així com algorismes eficients per tractar-los.

19.1 Representacions de grafs

Computacionalment, els grafs s'acostumen a emmagatzemar fent servir algun dels mètodes següents.

Llistes d'adjacència: Per a cada vèrtex, es llista els vèrtexos que són adjacents a ell. Aquesta descripció es pot fer servir tant per grafs no dirigits com dirigits.

Exemple: Considerem el graf de la figura i el seu diccionari de vèrtexos adjacents:



v	$\mathcal{A}(v)$
1	2,4
2	1,4,5
3	5
4	1,2
5	2,3

Matrius d'adjacència: S'enumeren els vèrtexos del graf $G = (V, E)$, $V = \{v_1, \ldots, v_n\}$, i es construeix la matriu $A = (a_{i,j})$ amb

$$a_{i,j} = \begin{cases} 1 & \text{si } v_i v_j \in E \\ 0 & \text{altrament.} \end{cases}$$

Aquesta matriu es pot generalitzar fàcilment a multigrafs, posant a $a_{i,j}$ el nombre d'arestes que uneixen v_i i v_j. Observem que la matriu que s'obté és simètrica i, suposant que el graf no té llaços, té zeros a la diagonal.

És immediat comprovar que donada la matriu, es pot recuperar el graf, enumerant n vèrtexos i posant entre els vèrtexos i i j el nombre d'arestes que marca l'entrada (i, j) de la matriu. Observem, però que la matriu canvia si es canvia l'ordenació dels vèrtexos. En particular, dos grafs són isomorfs si, i només si, existeixen ordenacions respectives dels seus vèrtexos tal que les matrius d'adjacència corresponents coincideixen.

Per al cas de digrafs, es pot fer servir la mateixa descripció, tenint ara en compte que la matriu que s'obtindrà no té perquè ser simètrica.

Exemple: Per al graf anterior, amb l'ordenació natural dels vèrtexos, la seva matriu d'adjacència és:

$$\begin{pmatrix} 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \end{pmatrix}$$

La matriu d'adjacència A ens dóna el nombre de camins de longitud 1 (és a dir, el nombre d'arestes) que uneixen els vèrtexos v_i i v_j. Les potències successives d'ella ens donen el nombre de recorreguts de longitud fixada entre nodes.

Proposició 33: *Sigui A^k la potència k-èssima de A, i diguem $a_{i,j}^{(k)}$ la seva entrada en la posició (i, j). Aleshores $a_{i,j}^{(k)}$ compta el nombre de recorreguts entre v_i i v_j de longitud k.*

PROVA: Fem la prova per inducció sobre k. El resultat és cert per definició per a $k = 1$. Suposem el resultat cert per a $k - 1$ i provem-lo per a k. Els camins de longitud k de v_i a v_j estan en bijecció amb els parells formats per un recorregut de longitud $k - 1$ de v_i a v_l i una aresta entre v_l i v_j (amb $v_l \in V$ qualsevol). Per tant, n'hi ha tants com:

$$\sum_{l=1}^{n} a_{i,l}^{(k-1)} a_{l,j}.$$

Ara, aquesta suma coincideix amb l'entrada (i, j) de $A^{k-1} \cdot A = A^k$. □

Matrius d'incidència: S'enumeren els vèrtexos i arestes del graf, $V = \{v_1, \ldots, v_n\}$, $E = \{e_1, \ldots, e_n\}$ i es construeix la matriu $B = (b_{i,j})$ amb

$$b_{i,j} = \begin{cases} 1 & \text{si } v_i \text{ és incident amb } e_j \\ 0 & \text{altrament.} \end{cases}$$

Per al cas de digrafs, s'enumeren els seus arcs i la matriu ve donada per

$$b_{i,j} = \begin{cases} 1 & \text{si } v_i \text{ és el vèrtex inicial de } e_j \\ -1 & \text{si } v_i \text{ és el vèrtex final de } e_j \\ 0 & \text{altrament.} \end{cases}$$

Exemple: Per a l'exemple anterior, la matriu d'incidència és

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Teorema 34: *Sigui G un graf qualsevol, A la seva matriu d'adjacència, B la seva matriu d'incidència i D la matriu diagonal amb entrades a la diagonal $d_i = d(v_i)$, totes elles amb la mateixa ordenació de vèrtexos. Aleshores,*

$$B \cdot B^t = A + D$$

PROVA: Diguem $V = \{v_1, \ldots, v_n\}$ i $E = \{e_1, \ldots, e_m\}$. Si $i \neq j$, l'entrada a la posició (i, j) de $B \cdot B^t$ és $\sum_{k=1}^{m} b_{i,k} b_{j,k}$ i cada producte és diferent de 0 únicament quan $e_k = v_i v_j$, i en tal cas, pren el valor 1. Així, la suma que apareix és igual a $a_{i,j}$. Ara, si $i = j$, l'entrada (i, i) de $B \cdot B^t$ és $\sum_{k=1}^{m} b_{i,k} b_{i,k}$ i cada producte és zero llevat que e_k sigui incident amb v_i, i en tal cas pren el valor 1; per tant, tenim que la suma obtinguda és igual al grau del vèrtex, $d(v_i)$. □

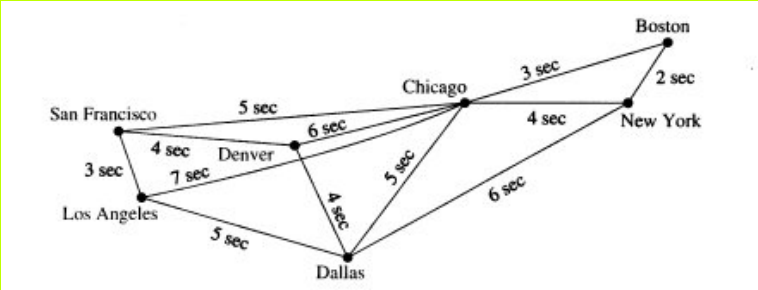
19.2 Algorismes sobre grafs

Un dels aspectes fonamentals dels grafs és que es fan servir per a modelar problemes i que existeixen algorismes per resoldre'ls basats en aquesta estructura de graf.

La majoria de llenguatges de programació d'alt nivell implementen grafs fent servir internament alguns dels mètodes de representació que hem descrit, i proporcionant procediments d'accés a l'estructura. En particular, es pot iterar sobre els nodes o arestes del graf, i sobre els vèrtexos adjacents a un de donat.

Com a exemple d'aquests algorismes considerem el problema dels camins mínims. Un graf *amb pesos* es un graf on cada aresta té assignada un *pes* positiu, és a dir, es té una funció $w : E \to \mathbb{R}^+$. Un cas particular és el pes trivial, on tota aresta té el mateix pes, que podem considerar unitari.

Exemple: El graf amb pesos següent representa el temps de transmisió d'un arxiu entre ordinadors situats a diferents ciutats.



El problema del camí mínim demana, donats dos vèrtexos d'un graf, quin es el camí que els uneix que té pes mínim, entès aquest com la suma dels pesos de les arestes que pertanyen al camí. Una solució a aquest problema el dóna l'algorisme de Dijkstra. De fet, aquest algorisme resol el problema per a un orígen fixat i simultàniament per a tots els destins possibles.

L'algorisme funciona mantenint una taula de *distàncies* i una taula de *predecessors* per a cada node del graf, així com una llista de nodes *optimitzats*, per als quals la solució trobada fins al moment és òptima. Així, en cada moment d'execució de l'algorisme, la taula de distàncies conté la distància mínima trobada fins al moment entre el node original i el node en qüestió, i la taula de predecessors conté el node anterior que es visita per arribar al node en qüestió pel camí òptim. Aquestes taules es van actualitzant fins a trobar una solució global.

Dades: Un graf G i un node orígen u.
NoOpt := V;
per a *tot node* v *diferent de* u **fer**
  dist(v) := ∞;
  pred(v) := nodef;
fi per a
dist(u) := 0;
mentre NoOpt $\neq \emptyset$ **fer**
  Sigui $v \in$ NoOpt amb dist(v) mínim;
  NoOpt := NoOpt $\setminus \{v\}$;
  per a *tot node* v' *de* NoOpt *adjacent a* v **fer**
    si dist(v) + $w(vv')$ < dist(v') **aleshores**
      dist(v') = dist(v) + $w(vv')$;
      pred(v') = v;
    fi si
  fi per a
fi mentre
Sortida: Taula amb dist(v) i pred(v)

A la pàgina web http://en.wikipedia.org/wiki/Dijkstra%27s_algorithm podeu trobar enllaços a animacions il·lustrant aquest algorisme, així com diferents demostracions.

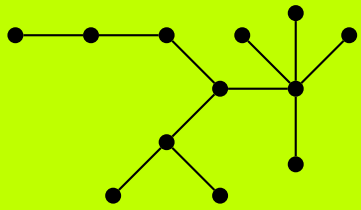
Lliçó 20

Arbres

20.1 Arbres no arrelats

Un *arbre* (no arrelat) és un graf no dirigit, connex i sense cicles.

Exemple:



Teorema 35: *Les següents condicions sobre un graf G són equivalents:*

1. *G és connex i acíclic.*
2. *Tot parell de vèrtexos de G està unit per un únic camí.*
3. *G és connex i, si el seu ordre és n, la seva mida és $n-1$.*
4. *G és connex, però $G-e$ és no connex per a tota aresta $e \in E(G)$.*
5. *G és acíclic, però $G+uv$ conté un cicle per a tot parell u, v de vèrtexos independents.*

Prova: (1) $\implies$ (2): L'existència de un camí ve donada pel fet que G és connex. Si n'existeixen dos de diferents, composant un qualsevol d'ells amb el que resulta d'invertir l'altre, s'obté un cicle.

(2) $\implies$ (1): La connexitat s'obté per l'existència de camins entre tot parell de vèrtexos. Suposem que G conté un cicle, i siguin u i v dos vèrtexos qualssevol d'aquest. Ara, el cicle es pot descomposar en dos camins, un de u a v i l'altre de v a u; invertint aquest segon, obtenim un camí de u a v diferent del primer, cosa que contradiu la hipòtesi.

(2) $\implies$ (3): El resultat és immediat per a $n = |V| = 1, 2, 3$. Suposem que el resultat és cert per a tot graf d'odre $k < n$, i sigui G un graf connex i acíclic d'ordre n. Sigui $e = uv$ una aresta qualsevol de G; el graf $G - e$ té dos components connexos, ja que u i v no poden estar units per un camí a $G - e$ (altrament hi hauria més d'un camí entre ells a G). Sigui T_u el component connex que conté u i T_v la que conté v. Aquests grafs són connexos i acíclics, i el seus ordres respectius n_u i n_v són menors que n, ja que $n_u + n_v = n$; per la hipòtesi d'inducció tenim que les seves mides són $m_u = n_u - 1$ i $m_v = n_v - 1$. Ara, com que $E(G) = E(T_u) \sqcup E(T_v) \sqcup \{e\}$, tenim que G té mida $m = m_u + m_v + 1 = n_u + n_v - 1 = n - 1$.

(3) $\implies$ (1): Vegem en primer lloc que G té almenys un vértex de grau 1; altrament, per ser connex, tot vèrtex tindria grau $\geqslant 2$ i, per tant, tindriem $2|E| = \sum_{u \in V} d(u) \geqslant 2n$ contra la hipòtesi que $|E| = n - 1$. Suposem ara que el resultat és cert per a tot graf d'ordre $k < n$; es a dir, si G' és un graf d'ordre $k < n$ i mida $k - 1$, aleshores G' és un arbre. Sigui G un graf d'ordre n i mida $n - 1$, i sigui u un vèrtex de grau 1; aleshores $G - u$ té ordre $n - 1$ i mida $n - 2$ (hem eliminat un únic vèrtex que té una única aresta incident); per hipòtesi d'inducció, $G - u$ és connex i acíclic, i G ho és també.

(1) $\implies$ (4): Suposem que $G - e$ és connex per a certa aresta $e = uv$. Aleshores, concatenant un camí entre u i v dins $G - e$ amb l'aresta e obtindriem un cicle a G, cosa que és impossible.

(4) $\implies$ (1): Suposem que G és connex i té un cicle C, i sigui e una aresta qualsevol del cicle. Aleshores $G - e$ és connex, ja que tot camí que passa per e es pot fer seguint el camí format per $C - e$.

(1) $\implies$ (5): Siguin u i v vèrtexos independents en un arbre, i sigui C l'únic camí que uneix u i v. Aleshores $C + uv$ forma un cicle de $G + uv$.

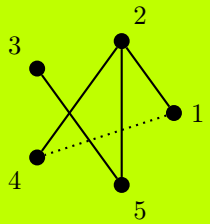
(5) $\implies$ (1): Si G no conté cicles, però per a tot parell de vèrtexos independents u i v, el graf $G + uv$ ja no és acíclic, aleshores G ha de ser connex, ja que altrament si u i v son vèrtexos de components connexos diferents, $G + uv$ no tindria cap cicle. □

Un graf es diu que és un *bosc* si els seus components connexos són arbres; és a dir, un bosc és un graf acíclic. Fent servir la descomposició en components connexos és immediat provar que si un bosc té n vèrtexos i k components connexos, aleshores té $n - k$ arestes.

20.2 Arbres generadors

Un *arbre generador* d'un graf connex G és un subgraf generador de G (és a dir, conté tots els seus vèrtexos) que és un arbre.

Exemple: En el graf de la figura s'indica quines arestes s'han de treure per obtenir un arbre generador.



Observem que un arbre generador T és un arbre maximal contingut a G, en el sentit que si afegim a T alguna aresta de G que no pertany a T, deixa de ser arbre per contenir algun cicle.

Teorema 36: *Tot graf connex té algun arbre generador.*

PROVA: Recordem que, per a tot graf connex amb n vèrtexos i m arestes, es compleix que $m \geqslant n-1$. Provarem el resultat per inducció sobre el nombre d'arestes del graf, sent el cas inicial $m = n-1$. Si $m = n-1$, tot graf d'ordre n i mida m és arbre (condició 3 del teorema de caracterització d'arbres) i, per tant, arbre generador d'ell mateix. Suposem el resultat cert per a grafs amb n vèrtexos i nombre d'arestes major o igual que $n-1$ i menor que m, i vegem que es compleix per a grafs amb n vèrtexos i m arestes. Sigui G un graf amb n vèrtexos i m arestes. Com que $m > n-1$, G necessàriament ha de contenir un cicle (altrament seria connex i acíclic, i tindriem $m = n-1$). Sigui e una aresta que forma part d'un cicle dins G. Eliminant l'aresta e s'obté el graf $G' = G - e$ amb $n' = n$ vèrtexos i $m' = m-1$ arestes. Per hipòtesi d'inducció, G' conté un arbre generador, que també ho és de G ja que $V' = V$. □

Un dels problemes d'optimització que es descriuen en termes de teoria de grafs és el de trobar arbres generadors minimals. Considerem, per exemple, una xarxa d'ordinadors amb un conjunt de possibles enllaços entre nodes, cadascun amb un preu fixat. Es tracta de trobar el conjunt d'enllaços de manera que tots els nodes estiguin connectats (no necessàriament de forma directa) i que el preu sigui mínim. En termes de teoria de grafs, donat un graf amb pesos a les arestes, es tracta de trobar un arbre generador del graf que tingui per pes total (definit com a la suma dels pesos de les arestes de l'arbre) el mínim possible.

Hi ha diferents algorismes que resolen aquest problema; veurem l'algorisme de Prim.

Dades: Un graf G amb pesos a les arestes.
Sigui n el nombre de vèrtexos de G;
Sigui $e = uv$ una aresta de G de pes minimal;
Sigui $V_1 := \{u, v\}$;
Sigui $T := (V_1, \{e\})$;
per a $k = 2, \ldots, n-1$ **fer**
  Sigui $e_k = (u_k v_k)$ de pes mínimal t.q. $u_k \in V_{k-1}$, $v_k \notin V_{k-1}$;
  Fem $V_k := V_{k-1} \cup \{v_k\}$;
  Fem $T := T + e_k$;
fi per a
Sortida: T

Proposició 37: *L'algorisme de Prim proporciona un arbre generador minimal.*

PROVA: El graf T que proporciona l'algorisme de Prim és un arbre, ja que és un graf connex amb n vèrtexos i $n-1$ arestes. Sigui T' un arbre generador minimal, i suposem que $T' \neq T$. Sigui $e = e_k = u_k v_k$ la primera aresta que s'obté en l'execució de l'algorisme i que no pertany a T'. Sigui P un camí des de u_k fins a v_k dins T'; anant recorrent P eventualment arribem a una aresta f que uneix un vèrtex de V_{k-1} amb un vèrtex que no pertany a V_{k-1}. Ara, atès que a la iteració k s'ha afegit e i no f, tenim que $w(f) \geqslant w(e)$. Sigui T'' el graf obtingut d'eliminar de T' l'aresta f i afegir l'aresta e. Fàcilment es veu que T'' és connex i té $n-1$ arestes; per tant, és un arbre i té pes no superior al de T'; per tant, és també un arbre generador minimal que, a més, conté totes les arestes de T afegides abans de e i també l'aresta e. Repetint el procediment obtenim un arbre generador minimal que és idèntic a T. □

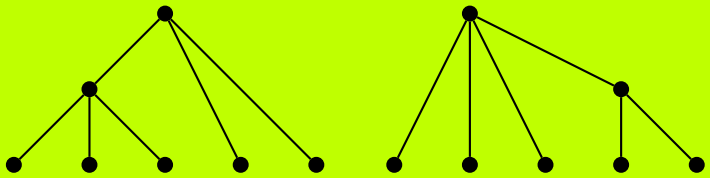
Lliçó 21

Arbres arrelats

21.1 Arbres arrelats

Un *arbre arrelat* (T, r) és un arbre T amb un vèrtex distingit r que s'anomena *arrel*. El fet de distingir un vèrtex s'ha d'entendre com que un isomorfisme d'arbres arrelats entre (T, r) i (T', r') és un isomorfisme de grafs entre T i T' que ha de portar necessàriament r a r'.

Exemple: Els arbres següents són isomorfs com a arbres, però no com a arbres arrelats.



Els arbres arrelats s'acostumen a representar gràficament amb l'arrel a dalt de tot, i amb els altres vèrtexos penjant cap a baix. Així, s'introdueix de manera natural una orientació en les arestes (que esdevenen arcs) en el sentit que s'allunyen de l'arrel. Més concretament, si $e = uv$ és una aresta de l'arbre (no arrelat), i $d(r, u) < d(r, v)$, aleshores uv és un arc del graf arrelat; altrament, ho és vu.

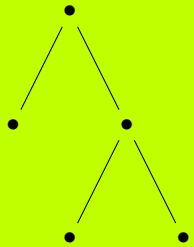
Així, equivalentment, un arbre arrelat és DAG amb un únic vèrtex r amb $d_e(r) = 0$ i tal que per a tot vèrtex $u \neq r$, existeix un únic camí de r a u. Això implica que tot vèrtex, llevat de r, té grau d'entrada 1.

En els arbres arrelats, sovint es fan servir notacions que provenen del llenguatge de l'evolució, on es fan servir. Així, si hi ha un arc de u a v, es diu que u és el *pare* de v, o que v és un *fill* de u; dos nodes es diu que són *germans* si tenen el mateix pare. Els nodes que són accessibles des d'un de donat es diu que formen la seva *descendència*, i aquells des dels quals es pot accedir al donat, la seva *ascendència*. Els nodes sense fills s'anomenen *fulles*, i els que si en tenen s'anomenen nodes *interiors*.

21.2 Arbres binaris

Un arbre arrelat es diu que és *binari* si tot node interior té dos fills.

Exemple:



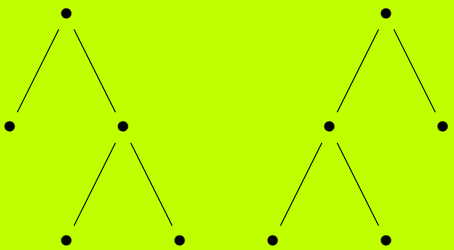
Observem que no hi ha arbres binaris arrelats de mida parell, com és lògic.

21.3 Arbres ordenats

Un arbre arrelat es diu *ordenat* (o *pla* o *lineal*) si es fixa, per a cada node interior, una ordenació dels seus fills. Aquesta ordenació s'ha d'entendre a nivell d'isomorfisme; és a dir, un isomorfisme d'arbres ordenats és un isomorfisme d'arbres arrelats tal que la imatge de la successió ordenada de fills d'un node coincideix amb la successió ordenada dels fills del node imatge.

Els arbres ordenats es representen de manera que els fills d'un determinat node apareixen d'esquerra a dreta segons l'ordenació fixada.

Exemple: Els arbres arrelats següents són isomorfs com a arbres arrelats, però no com a arbres ordenats.



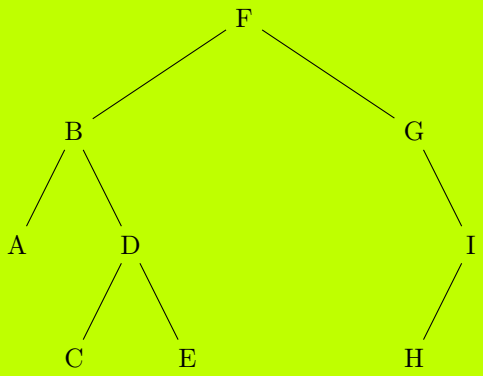
21.4 Recorreguts sobre arbres

Els arbres arrelats sovint es fan servir per emmagatzemar informació als nodes i, per tant, és interessant de tenir diferents maneres de visitar tots els nodes.

Considerem el cas d'arbres binaris ordenats. El tractament d'un arbre es basa en dues operacions: visitar l'arrel i tractar subarbres penjant de l'arrel. L'ordre en que es facin aquestes operacions determina diferents ordenacions.

- Recorregut en preordre de T:
  1. Visitar l'arrel de T.
  2. Recorre en preordre el subarbre de l'esquerra de T.
  3. Recorre en preordre el subarbre de la dreta de T.
- Recorregut en inordre de T:
  1. Recorre en inordre el subarbre de l'esquerra de T.
  2. Visitar l'arrel de T.
  3. Recorre en inordre el subarbre de la dreta de T.
- Recorregut en postordre de T:
  1. Recorre en postordre el subarbre de l'esquerra de T.
  2. Recorre en postordre el subarbre de la dreta de T.
  3. Visitar l'arrel de T.

Exemple: Considerem l'arbre següent:



L'ordre en que es van visitant els nodes en cada recorregut és:

- Preordre: F, B, A, D, C, E, G, I, H.
- Inordre: A, B, C, D, E, F, G, H, I.
- Postordre: A, C, E, D, B, H, I, G, F.

En cas de tenir arbres no binaris, els recorreguts en preordre i postordre es generalitzen de manera natural; el recorregut en inordre presenta el problema de decidir entre quins dos subarbres a recorre es visita l'arrel, tot i que sovint s'escull fer-ho entre el primer i el segon subarbre recorregut.

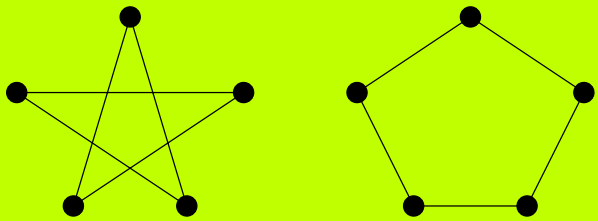
Lliçó 22

Planaritat

22.1 Grafs planars

Un graf es diu *planar* si, intuitivament, es pot dibuixar en el pla de manera que les seves arestes no es tallen. Un tal dibuix es diu que és una *representació plana* del graf. Observem que el fet de donar una representació no plana no implica que no n'existeixi una de plana.

Exemple: A la figura següent hi ha dues representacions del mateix graf. Per tant, el graf de l'esquerra és planar.



Per tal de provar que un graf és planar n'hi ha prou en trobar-ne una representació plana. En canvi, per provar que no ho és hem de fer servir criteris que no depenguin de la representació donada.

22.2 Criteris numèrics

Suposem donada una representació plana d'un graf. Una *cara* del graf és una regió del pla delimitada per arestes del graf. Observem que una representació plana del graf divideix el pla en cares, i que una d'elles és infinita, la *cara exterior*, que s'ha de tenir en compte. Indicarem per F el conjunt de cares d'un graf (en el benentès que depèn, en principi, de la representació plana donada).

Teorema 38 (Equació d'Euler): *Tot graf planar connex compleix que*

$$|V| - |E| + |F| = 2.$$

PROVA: Si $|V| = 1$, totes les arestes són llaços, i el nombre de cares és $|F| = |E| + 1$, d'on s'obté el resultat. Suposem el resultat cert per a grafs amb nombre d'arestes menor que n i vegem que també es compleix per a grafs amb n vèrtexos. Sigui G un graf amb n vèrtexos i sigui e una aresta que connecta dos vèrtexos diferents i considerem G' el graf obtingut per contracció d'aquesta aresta. El graf G' té $|F'| = |F|$ cares, $|E'| = |E| - 1$ arestes i $|V'| = |V| - 1$ vèrtexos. Per hipòtesi d'inducció es té que $|V'| - |E'| + |F'| = 2$, d'on s'obté que $|V| - |E| + |F| = 2$, com volíem provar.□

Alguns criteris que es poden fer servir per a provar la no-planaritat són els següents.

Proposició 39: *Sigui G un graf simple, connex i planar. Aleshores:*

1. $2|E| \geqslant 3|F|$,
2. $3|V| - |E| \geqslant 6$.
3. *G té algun vèrtex de grau menor o igual que* 5.
4. *Si G no té circuits de longitud* 3, *aleshores* $|E| \leqslant 2|V| - 4$.

PROVA:

1. Per a cada cara del graf, diguem el seu *grau* el nombre d'arestes que el delimiten. De la hipòtosesi que el graf és simple, es segueix que totes les cares tenen grau com a mínim 3, d'on se segueix que la suma dels graus de les regions és com a mínim $3|F|$. Per altra banda, cada aresta pertany a la frontera d'exactament dues regions; per tant, la suma dels graus de les regions és igual a $2|E|$, d'on tenim que $2|E| \geqslant 3|F|$.
2. Fent servir que $|F| = |E| + |V| + 2$ i el resultat anterior, obtenim que $|E|/3 \leqslant |V| - 2$, d'on es dedueix el resultat.
3. El tercer resultat és clarament cert per a grafs amb 1 o 2 vèrtexos. Si G té com a mínim 3 vèrtexos, pel resultat anterior tenim que $2|E| \leqslant 6|V| - 12$. Si el grau de tots els vèrtexos fos com a mínim 6, pel lema de les encaixades, tindriem que $2|E| \geqslant 6|V|$, que entra en contradicció amb la desigualtat anterior.
4. La quarta propietat es dedueix de manera anàloga a la segona, tenint en compte que les cares tindran grau com a mínim 4. □

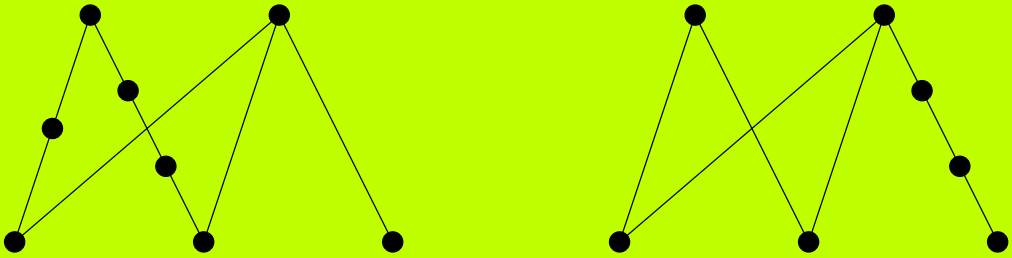
Exemple: Dels resultats anteriors es dedueix que els grafs K_5 i $K_{3,3}$ no són planars. De fet, aquests són els grafs "més senzills" que no ho són.

22.3 Teorema de Kuratowski

Sigui G un graf i $e = uv$ una aresta. El graf que resulta d'eliminar l'aresta e, afegir un nou vèrtex w i les arestes uw i wv, es diu que s'ha obtingut de G per *subdivisió elemental*. Intuitivament,

consiteix en afegir un vèrtex al mig d'una aresta. Dos grafs es diuen *homeomorfs* si tots dos es poden obtenir a partir d'un mateix graf per mitjà d'una seqüència de subdivisions elementals.

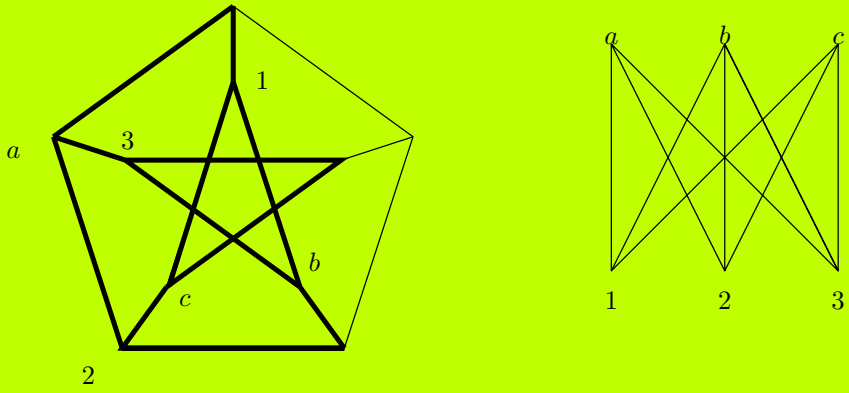
Exemple: Els grafs següents són homeomorfs.



Teorema 40: *Un graf és no planar si, i només si, conté un subgraf homeomorf a $K_{3,3}$ o a K_5.*

Aquest resultat, que no provarem, ens diu que els grafs $K_{3,3}$ i K_5 són els "blocs constituents" dels grafs no planars.

Exemple: El graf de Petersen no és planar. A continuació es dóna aquest graf, junt amb un subgraf homeomorf a $K_{3,3}$.

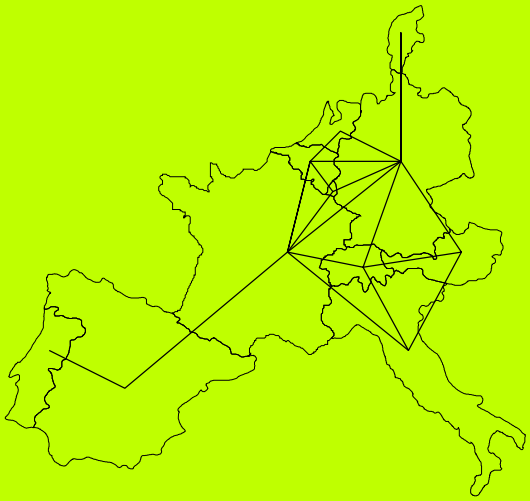


Lliçó 23

Grafs colorejats

L'origen dels grafs colorejats és el problema de coloració de mapes. Es té un pla dividit en regions, i es vol pintar les regions de colors, de manera que les regions que comparteixen frontera estiguin pintades de colors diferents. A una tal situació se li assigna un graf, on els vèrtexos són les regions, i dos vèrtexos estan units per una aresta si, i només si, les regions corresponents comparteixen frontera.

Exemple:



Una *coloració* d'un graf G és una aplicació f de V en un conjunt $C = \{1, \ldots, k\}$ de *colors*. Una coloració es diu *pròpia* si vèrtexos adjacents tenen colors diferents; és a dir, si $uv \in E$ aleshores $f(u) \neq f(v)$. Un graf es diu que és *k-colorejable* si admet una coloració pròpia amb k colors. El nombre cromàtic d'un graf G s'indica per $\chi(G)$ i és el més petit k tal que G és k-colorejable.

Exemple:

- El nombre cromàtic de L_n és 2.
- El nombre cromàtic de C_n és 2 si n és parell i 3 si n és senar.

- El nombre cromàtic de K_n és n.

Observem que el nombre cromàtic d'un graf amb n vèrtexos és, com a molt, n, i que hi ha grafs amb n vèrtexos i amb nombre cromàtic n (el graf complet K_n té nombre cromàtic n). En canvi, si ens restringim a grafs planars (que són aquells per als que té sentit la interpretació que motiva el problema) aquest nombre és com a molt 4.

Teorema 41 (Teorema dels 4 colors): *El nombre cromàtic d'un graf planar és, com a molt,* 4.

Aquest teorema, que no provarem, va ser demostrat per primera vegada l'any 1976, després d'un seguit de demostracions falses, i requereix una exhaustiva comprovació de més de 2000 casos, que van ser comprovats per ordinador.

Una manera de calcular el nombre cromàtic d'un graf és a través del seu *polinomi cromàtic*. Donat un graf G, i un enter k, sigui $P_G(k)$ el nombre de k-coloracions pròpies de G.

Exemple:

- El polinomi cromàtic de L_n és $k(k-1)^{n-1}$.
- El polinomi cromàtic de C_n és $(k-1)^n + (-1)^n(k-1)$.
- El polinomi cromàtic de K_n és $k(k-1)\dots(k-(n-1))$.

El següent resultat dóna una manera recursiva de calcular $P_G(k)$ i, en particular, prova que $P_g(k)$ és, de fet, un polinomi en la variable k.

Proposició 42: *Sigui G un graf.*

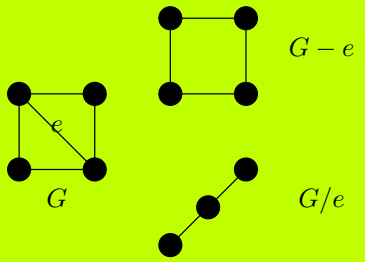
1. *Si G descomposa en components connexos, $G = G_1 \sqcup G_2 \sqcup \cdots \sqcup G_m$, es té que*
$$P_G(k) = P_{G_1}(k) \cdot P_{G_2}(k) \cdots P_{G_m}(k).$$
2. *Si $e = uv$ és una aresta de G, $G - e$ el graf resultant d'eliminar l'aresta e i G/e el graf que resulta de contraure l'aresta e, es té que*
$$P_G(k) = P_{G-e}(k) - P_{G/e}(k).$$

PROVA: 1. Ja que cap vèrtex de G_i és adjacent a cap vèrtex de G_j $(i \neq j)$, es té que les k-coloracions de G estan en bijecció amb el producte cartesià de les k-coloracions dels grafs G_i i, per tant, el cardinal de les primeres és igual al producte dels cardinals.

2. Considerem el conjunt de k-coloracions de $G-e$. Si una tal coloració assigna colors diferents als extrems de e, aleshores és una k-coloració de G; altrament, els vèrtexos u i v tenen el mateix color i, per tant, indueix una coloració pròpia del graf quocient G/e. Recíprocament, tota k-coloració de G, indueix una coloració de $G-e$ on u i v tenen colors diferents, i tota k-coloració de G/e indueix una coloració de $G-e$ on u i v tenen el mateix color. Atès que aquests conjunts de coloracions són disjunts, tenim que $P_{G-e}(k) = P_G(k) + P_{G/e}(k)$. □

Observem que el nombre cromàtic d'un graf és el més petit enter positiu k amb $P_G(k) \neq 0$.

Exemple: Considerem el graf de la figura, amb l'aresta indicada i els subgrafs i grafs quocients que apareixen.



Es té que

$$P_G(k) = P_{G-e}(k) - P_{G/e}(k) = (k-1)^4 + (k-1) - k(k-1)^2 = k(k-1)(k-2)^2$$

en particular, el seu nombre cromàtic és 3.