

Capítol 1 : Conceptes bàsics

Matemàtica discreta
Grau d'Enginyeria Informàtica
Escola d'Enginyeria
Universitat Autònoma de Barcelona

- 1 Conjunts i operacions amb conjunts
- 2 Producte cartesià i relacions binàries
- 3 Elements de combinatòria
- 4 Conjunts finits, infinits i numerables
- 5 Complexitat d'algorismes i problemes
- 6 Funcions de complexitat

Conjunts i operacions amb conjunts

Un **conjunt** és una colla d'elements sense repeticions i sense ordre. Normalment denotem els conjunts amb lletres majúscules i els elements entre claus. Per exemple, $A = \{a, b, c\}$. A més, utilitzem les següents notacions:

$a \in A$ (l'element a pertany al conjunt A)

$\{a, b\} \subset A$ ($\{a, b\}$ està inclòs a A , $\{a, b\}$ és un subconjunt de A)

$\{a, b\} \subseteq A$ (és el mateix remarquant que es pot donar la igualtat)

$\{a, b\} \subsetneq A$ ($\{a, b\}$ està estrictament inclòs a A).

Tenim, en canvi, $d \notin A$, $\{c, d\} \not\subseteq A$.

Conjunts i operacions amb conjunts

De vegades, no escrivim tots els elements:

$$B = \{1, \dots, 9\}; \quad B = \{n \in \mathbb{N} \mid 1 \leq n \leq 9\};$$

$$\mathbb{N} = \{1, 2, \dots\} = \{n \in \mathbb{Z} \mid n > 0\}.$$

El nombre d'elements d'un conjunt finit X o **cardinal** el denotarem per $|X|$, $\#X$ o $Card(X)$.

Definim el **conjunt buit** $\emptyset$ com aquell que no té cap element:

$|\emptyset| = 0$. De la teoria axiomàtica de conjunts es dedueix l'existència i unicitat del conjunt buit. També s'arriba a la conclusió que $\emptyset \subset A$, per a tot conjunt A .

Conjunts i operacions amb conjunts

Definim les següents operacions entre conjunts:

- (i) *Unió o reunió*: $A \cup B = \{x \mid x \in A \text{ i/o } x \in B\}$.
- (ii) *Intersecció*: $A \cap B = \{x \mid x \in A \text{ i } x \in B\}$.
- (iii) *Complementació*: $\overline{A} = A^c = \{x \mid x \notin A\}$.
- (iv) *Resta*: $A \setminus B = \{x \mid x \in A \text{ i } x \notin B\}$.

Per a la complementació, és evident que cal tenir un conjunt de referència dintre del qual estan tots els elements que considerem. Així, si $A = \{1, 2\}$ i el nostre conjunt de referència fos $\mathbb{N}$, tindríem que $\overline{A} = \{n \in \mathbb{N} \mid n > 2\}$.

Conjunts i operacions amb conjunts

Les següents propietats són evidents a partir de les definicions de les operacions:

- (i) La unió i la intersecció de conjunts són operacions associatives i commutatives.
- (ii) La unió i la intersecció de conjunts són operacions idempotents: $A \cup A = A \cap A = A$, per a tot conjunt A .
- (iii) El complementari del complementari d'un conjunt és ell mateix: $\overline{\overline{A}} = A$, per a tot conjunt A .
- (iv) Per a tot conjunt A , es verifica: $A \cup \emptyset = A$, $A \cap \emptyset = \emptyset$, $A \setminus \emptyset = A$, $A \setminus A = \emptyset$.

Una altra propietat interessant és que $A \setminus B = A \cap \overline{B}$.

També es poden comprovar fàcilment les *lleis de De Morgan*:

$$\overline{A \cup B} = \overline{A} \cap \overline{B}; \quad \overline{A \cap B} = \overline{A} \cup \overline{B}.$$

Respecte al *cardinal* de conjunts finits, tenim que

$|A \cup B| = |A| + |B| - |A \cap B|$, on A i B són finits. La fórmula pot generalitzar-se per a la unió de més de dos conjunts.

Conjunts i operacions amb conjunts

Si A és un conjunt, llavors es defineix el **conjunt de les parts** de A com el conjunt de tots els subconjunts de A . Ho denotem per $\mathcal{P}(A)$ o bé 2^A .

Exemple 1.

Si $A = \{1, 2\}$, llavors $\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$.

Notem que ara, excepcionalment, tenim notacions com $\emptyset \in \mathcal{P}(A)$ i $\{1\} \in \mathcal{P}(A)$ (però $\emptyset \subset A$ i $\{1\} \subset A$).

Si A és finit, llavors $|\mathcal{P}(A)| = 2^{|A|}$. La demostració es pot fer de diverses maneres com veurem en un exercici.

Siguin A i B conjunts, aleshores el **producte cartesià** $A \times B$ és el conjunt de totes les parelles ordenades, on el primer element és de A i el segon és de B :

$$A \times B = \{(a, b) \mid a \in A, b \in B\}.$$

Si A i B són finits, aleshores és clar que $|A \times B| = |A| \cdot |B|$.

Una **relació (binària)** R sobre un conjunt X és un subconjunt del producte cartesià de X per ell mateix:

$$R \subseteq X^2 = X \times X.$$

Si $x, y \in X$, diem que x està relacionat amb y si $(x, y) \in R$.
També es posa xRy .

Una relació $R \subseteq X^2$ és:

- (i) *Reflexiva* si $(x, x) \in R, \forall x \in X$.
- (ii) *Simètrica* si $((x, y) \in R \iff (y, x) \in R, \forall x, y \in X)$.
- (iii) *Transitiva* si $((x, y) \in R, (y, z) \in R \implies (x, z) \in R, \forall x, y, z \in X)$.

Una relació es diu d'**equivalència** si és (i), (ii) i (iii).

Les relacions d'equivalència, sovint es denoten amb el símbol $\sim$ i $(x, y) \in R$ (o xRy) també s'escriu $x \equiv y$ o $x \sim y$. Es diu que x i y són equivalents.

Exemple 2.

Examinem les següents relacions definides sobre els nombres enters:

- “ $\leq$ ” és (i) i (iii).
- “ $=$ ” és d'equivalència.
- “tenir la mateixa paritat” és d'equivalència.
- “no dividir a ” no és (i), ni (ii), ni (iii).

Si R és d'equivalència, diem *classe* a cada subconjunt d'elements relacionats entre si. Aquestes **classes d'equivalència** formen una partició de X . El conjunt de les classes d'equivalència es diu el **conjunt quocient** X/R , $X/\equiv$ o $X/\sim$, segons com denotem la relació.

Exemple 3.

Sigui X el conjunt dels europeus i considerem la relació $\sim$ "ser del mateix estat". Aleshores les classes son: francesos, italians, alemanys, etc.

En realitat, moltes vegades estem parlant de conjunts quocients sense adonar-nos-en. De fet, tota partició d'un conjunt, indueix una relació d'equivalència sobre el conjunt.

Aplicacions

Siguin A i B conjunts. Una **correspondència** assigna algun(s) o cap element de A a algun(s) o cap element de B . Més formalment, diríem que una correspondència és un subconjunt de $A \times B$.

Una tal correspondència es diu **aplicació**, denotada $f : A \longrightarrow B$ si a cada element de A li correspon un element de B . Essent $a \in A$, l'element corresponent de B es denota per $f(a)$. O sigui que s'ha de verificar:

$$f(a) \in B \quad \forall a \in A.$$

Definició 1.

Sigui $f : A \longrightarrow B$ una aplicació.

- (i) *La imatge d'un element $a \in A$ és $f(a)$.*
- (ii) *La imatge de A per f és*
$$f(A) = \text{Im } f = \{b \in B \mid \exists a \in A : f(a) = b\}.$$
- (iii) *L'antiimatge de $b \in B$ és $f^{-1}(b) = \{a \in A \mid f(a) = b\}$.*
Observem que $f^{-1}(b) \subseteq A$.

Definició 2.

Sigui $f : A \longrightarrow B$ una aplicació.

- (i) f és injectiva si $|f^{-1}(b)| \leq 1, \forall b \in B$.*
- (ii) f és exhaustiva o epijectiva si $|f^{-1}(b)| \geq 1, \forall b \in B$.*
- (iii) f és bijectiva si és (i) i (ii).*

Les següents propietats són evidents i, sovint, un les utilitza per demostrar que una aplicació és d'un determinat tipus.

- (i) f és injectiva si, i només si,
 $(f(a) = f(a') \implies a = a', \forall a, a' \in A)$.*
- (ii) f és exhaustiva si, i només si, $Im f = B$.*
- (iii) f és bijectiva si, i només si, $f^{-1} : B \longrightarrow A$ pot considerar-se una aplicació.*

Si A i B són finits, llavors, respecte als cardinals, podem assegurar que:

- Si f és injectiva, llavors $|A| \leq |B|$.
- Si f és exhaustiva, llavors $|B| \leq |A|$.
- Si f és bijectiva, llavors $|A| = |B|$.
- També és fàcil deduir, per exemple, que si f és injectiva i $|A| = |B|$, llavors f també és bijectiva.

Regla del producte

Si en una selecció tenim n_1 opcions en el primer pas, n_2 opcions en el segon pas, ..., n_k opcions en el pas k ; aleshores el nombre total de possibles seleccions en k passos és $n_1 \cdot n_2 \cdots n_k$.

Exemple 4.

- (i) *Quin és el nombre de cadenes binàries de longitud 3?*
- (ii) *Quin és el nombre de cadenes decimals de longitud 4, de forma que tots els dígits són diferents?*
- (iii) *Si tenim 3 noies i 2 nois, quantes parelles (de diferent sexe) es poden fer?*

Regla de la suma

Si tenim k conjunts disjunts d'objectes amb cardinals $n_1, \dots, n_k$ i hem de seleccionar un objecte, ho podem fer de $n_1 + \dots + n_k$ maneres diferents.

Exemple 5.

Si hem d'escollir una persona d'entre les 3 noies i els 2 nois, de quantes maneres ho podem fer?

Exemple 6.

Tenim 10 llibres en anglès, 8 en català i 6 en francès. Volem seleccionar 2 llibres que estiguin escrits en llengua diferent. Quantes opcions tenim?

El **factorial** d'un nombre enter n és

$$n! = n(n-1) \cdots 1, \text{ si } n > 0 \quad \text{i} \quad 0! = 1.$$

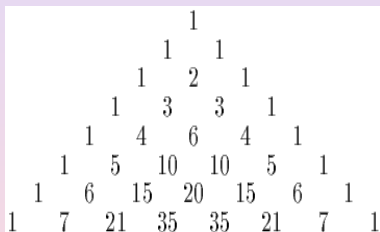
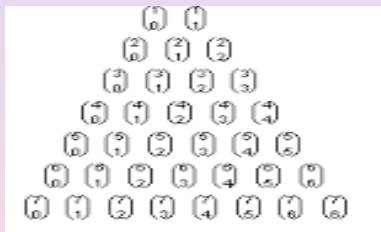
Si $k \leq n$ amb $k, n \geq 0$, llavors el **nombre combinatori** $\binom{n}{k}$ és

$$\binom{n}{k} = \frac{n(n-1) \cdots (n-k+1)}{k!} = \frac{n!}{k!(n-k)!} = \binom{n}{n-k}.$$

Propietats (demostració a classe de problemes):

- $\binom{n}{k} = \binom{n}{n-k}$
- $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$
- $\sum_{k=0}^n \binom{n}{k} = 2^n$

Nombres combinatoris calculats de forma recursiva per a $0 \leq n \leq 7$.



Donat un conjunt amb $n > 0$ objectes, en volem triar k .

Sense repetició ($k \leq n$) i importa l'ordre.

- Hi ha $n(n-1) \cdots (n-k+1) = \frac{n!}{(n-k)!}$ maneres diferents.
- S'anomenen **variacions sense repetició**.
- Coincideix amb el nombre d'aplicacions injectives d'un k -conjunt a un n -conjunt.

Exemple 7.

- (i) Si volem treure 3 cartes consecutivament (sense retornar-les) d'un joc de 48 cartes, quantes possibilitats diferents tenim?
- (ii) Si volem asseure 3 persones i tenim 10 cadires numerades, de quantes maneres diferents ho podem fer?

Donat un conjunt amb $n > 0$ objectes, en volem triar k .

Amb repetició i importa l'ordre.

- Hi ha $n \cdot n \cdots n = n^k$ maneres diferents.
- S'anomenen **variacions amb repetició**.
- Coincideix amb el nombre d'aplicacions d'un k -conjunt a un n -conjunt.

Exemple 8.

(i) Si volem treure 3 cartes consecutivament, retornant-les al munt cada vegada, quantes possibilitats diferents tenim?

(ii) Si volem assignar 8 pacients a 5 doctors –sense cap restricció– de quantes maneres diferents ho podem fer?

Donat un conjunt amb $n > 0$ objectes, en volem triar k .

Sense repetició, importa l'ordre i $n = k$.

- Hi ha $n(n-1) \cdots 1 = n!$, aplicant (i) per a $k = n$.
- S'anomenen **permutacions**.
- Coincideix amb el nombre de bijeccions entre dos n -conjunts. Quan els dos conjunts són el mateix, d'aquestes bijeccions també se'n diu permutacions.

Exemple 9.

- (i) Si estenem consecutivament totes les cartes, quantes ordenacions possibles tenim?
- (ii) Tenim els símbols $1, 2, 3, a, b, c$. Quantes cadenes de longitud 3 podem fer, sense repeticions i de forma que els tres símbols siguin tots nombres o tots lletres?

Tenim m tipus d'objectes, en volem triar r_1 del tipus 1, r_2 del tipus 2, ..., r_m del tipus m ($r_1 + \dots + r_m = n$).

Amb algunes repeticions, importa l'ordre i $n = k$.

- Hi ha $\frac{n!}{r_1! \dots r_m!}$ maneres diferents.
- S'anomenen **permutacions amb repetició**.
- Coincideix amb el nombre d'aplicacions exhaustives f d'un n -conjunt a un m -conjunt $B = \{b_1, \dots, b_m\}$ amb la condició que $|f^{-1}(b_j)| = r_j$, per tot $j = 1, \dots, m$.

Exemple 10.

(i) Si considerem totes les ordenacions possibles de les cartes però només tenint en compte els pals, quantes possibilitats diferents tenim?

(ii) De quantes maneres diferents podem ordenar les lletres de la paraula CAVALL?

Sense repetició ($k \leq n$) i no importa l'ordre.

Diguem $C(n, k)$ al nombre de possibilitats. Si comptés l'ordre, ja sabem que tindríem $\frac{n!}{(n-k)!}$ possibilitats. Per tant,

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

- S'anomenen **combinacions**.
- Coincideix amb el nombre de k -subconjunts d'un n -conjunt.
- Observem que sumant tots els subconjunts possibles d'un conjunt finit A amb cardinal n , obtenim:

$$|\mathcal{P}(A)| = \sum_{k=0}^n \binom{n}{k} \quad (= 2^n).$$

Exemple 11.

(i) Si volem seleccionar una parella de cartes (sense ordre ni retorn), llavors quantes possibilitats tenim?

(ii) Tenim un grup de 5 noies i un grup de 4 nois. Hem d'escollir dos representants de cada sexe. De quantes maneres ho podem fer?

Elements de combinatòria (vi)

Tenim n tipus d'objectes (nombre il·limitat de cada tipus) i n'hem de seleccionar k (pot ser que $k \geq n$).

Amb repetició i no importa l'ordre.

Exemple 12.

*Suposem que tenim gelats de maduixa, de llimona i de taronja. De quantes maneres podem seleccionar 9 gelats? Es pot transformar en un problema de permutacions amb repetició utilitzant el **model d'estrelles i barres**:*

$$\underbrace{***}_{\text{maduixa}} \mid \underbrace{**}_{\text{llimona}} \mid \underbrace{****}_{\text{taronja}}$$

En general, tindrem k estrelles i $n - 1$ barres. Per tant,

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

- S'anomenen **combinacions amb repetició**.

Considerem el conjunt dels nombres naturals $\mathbb{N} = \{1, 2, 3, \dots\}$.

Definició 3.

*Un conjunt X és **finit** si:*

- (i) $X = \emptyset$ (en tal cas, $|X| = 0$), o bé
- (ii) existeix una bijecció entre X i $\{1, \dots, n\}$, per a algun $n \in \mathbb{N}$ (en tal cas, $|X| = n$).

Definició 4.

*Un conjunt és **infinit** si no és finit.*

Lema 1.

Siguin X i Y dos conjunts tals que $X \subset Y$. Aleshores

- (i) Si Y és finit, llavors X és finit i, a més, $|X| \leq |Y|$.*
- (ii) Si X és infinit, llavors Y és infinit.*

Diferenciarem dos tipus de conjunts infinits: els numerables i els no numerables.

Definició 5.

*Dos conjunts infinits tenen la mateixa **cardinalitat** si existeix una bijecció entre ells.*

Definició 6.

*Un conjunt es diu **numerable** (enumerable o comptable) si és finit o té la mateixa cardinalitat que $\mathbb{N}$.*

Si A és un conjunt infinit numerable, llavors tenim una bijecció $f : \mathbb{N} \longrightarrow A$. Per tant, podem identificar els elements de A com $f(1), f(2), \dots$. Posant $a_k = f(k)$, podem escriure $A = \{a_1, a_2, \dots\}$. És a dir, podem enumerar els elements de A .

Remarca 1.

- (i) *En alguns texts, quan es parla de conjunts numerables, es vol dir sempre conjunts infinits numerables. Atès que els elements d'un conjunt finit sempre els podem enumerar, en aquest document el terme numerable inclou també el cas finit.*
- (ii) *Un conjunt discret està format per punts aïllats. Per exemple, $\mathbb{N}$ i $\mathbb{Z}$ són conjunts discrets. Qualsevol conjunt finit també és discret. Tot conjunt discret és numerable. Però hi ha conjunts numerables no discrets, per exemple, el conjunt dels nombres racionals $\mathbb{Q}$.*

Com que la composició de dues bijeccions és una bijecció, tenim que si volem demostrar que un cert conjunt infinit és numerable, només cal trobar una bijecció amb un altre conjunt infinit que ja sapiguem que és numerable, no cal que sigui $\mathbb{N}$.

Exemple 13.

Sigui $A = \mathbb{N} \cup \{0\}$. Definim l'aplicació:

$$\begin{aligned} f : A &\longrightarrow \mathbb{N} \\ n &\longrightarrow n + 1 \end{aligned}$$

Clarament f és bijectiva i, per tant, A és numerable. Semblaria que A té "un element més" que $\mathbb{N}$ però la realitat és que els dos conjunts són infinits i tenen la mateixa cardinalitat. Observem que els elements de A es poden enumerar fàcilment: $0, 1, 2, \dots$

Exemple 14.

Definim l'aplicació:

$$\begin{aligned} g : A &\longrightarrow \mathbb{Z} \\ n &\longrightarrow \begin{cases} (n+1)/2 & \text{si } n \text{ senar} \\ -n/2 & \text{si } n \text{ parell} \end{cases} \end{aligned}$$

Com que g és bijectiva, resulta que $\mathbb{Z}$ és numerable. En aquest cas, semblaria que $\mathbb{Z}$ té el doble (més o menys) d'elements que A , però podem enumerar els enters: $0, 1, -1, 2, -2, \dots$

Conjunts finits, infinits i numerables

Observem que si X és numerable i $X \subset Y$, llavors Y pot ser numerable o no: $\mathbb{N} \subset \mathbb{Z}$, $\mathbb{N} \subset \mathbb{R}$.

Lema 2.

Siguin X i Y dos conjunts tals que $X \subset Y$. Si Y és numerable, llavors X és numerable.

Corol·lari 1.

Si $f : X \rightarrow Y$ és injectiva i Y és numerable, llavors X és numerable.

El corol·lari anterior és molt útil, ja que ens diu que si volem demostrar que un cert conjunt A és numerable, n'hi ha prou amb trobar una injecció entre A i el conjunt dels nombres naturals o qualsevol altre conjunt numerable.

Exemple 15.

Definim l'aplicació:

$$\begin{aligned} f : \quad \mathbb{N} \times \mathbb{N} &\longrightarrow \mathbb{N} \\ (a, b) &\longrightarrow 2^a 3^b \end{aligned}$$

És fàcil comprovar que f és injectiva. Per tant, $\mathbb{N} \times \mathbb{N}$ és numerable.

Si A i B són conjunts numerables, llavors $A \times B$ és numerable. Aleshores $\mathbb{Z} \times \mathbb{Z}$, $\mathbb{Z} \times \mathbb{N}$, $\mathbb{Z}^k$, etc. són tots numerables. Tenim que existeix una injecció $\mathbb{Q} \longrightarrow \mathbb{Z} \times \mathbb{N}$. Per tant, $\mathbb{Q}$ és numerable.

Anem a veure ara conjunts no numerables.

Definició 7.

*Sigui $A = \{a_1, \dots, a_n\}$ i $B \subset A$. El **vector característic** de B és $v_B = (v_1, \dots, v_n)$, on $v_i = 1$ si $a_i \in B$ i $v_i = 0$ si $a_i \notin B$.*

Exemple 16.

Si $B = \emptyset$, llavors v_B és el vector tot zeros. En canvi, si $B = A$, llavors v_B és el vector tot uns.

Si A és finit, podem identificar $\mathcal{P}(A)$ amb el conjunt de tots els vectors binaris de n coordenades. Si A és infinit numerable, llavors podríem fer el mateix i identificar $\mathcal{P}(A)$ amb el conjunt de tots els vectors binaris amb infinites coordenades.

Exemple 17.

Si $A = \mathbb{N}$ i $B = \{n \in \mathbb{N} \mid n = 2k, k \in \mathbb{N}\}$, llavors tindríem $v_B = (0, 1, 0, 1, 0, 1, \dots)$.

Teorema 1.

Si A és infinit numerable, llavors $\mathcal{P}(A)$ és infinit no numerable.

Corol·lari 2.

$\mathbb{R}$ no és numerable.

Naturalment, tampoc seran numerables $\mathbb{C}$, $\mathbb{R}^n$, $\mathbb{C} \times \mathbb{R}$, etc.

Acabem dient que amb conjunts no numerables poden passar coses sorprenents com, per exemple, que $\mathbb{R}$ i $(0, 1) \subset \mathbb{R}$ tenen la mateixa cardinalitat.

Quan executem un programa (algorisme) tenim un cost en *temps* i *espai*. Això és la **complexitat (computacional) de l'algorisme**.

La complexitat sempre es mesura en funció de la mida de les *dades d'entrada* (nombre de vèrtexs, nombre d'ítems a ordenar, etc.), no interessa per a un cas particular ja que llavors no es veu com creix la complexitat en funció de com creix la mida de les dades.

La **complexitat d'un problema** és la complexitat del millor algorisme que el resol. Així si A és un algorisme que resol un problema P , sempre tindrem $C(P) \leq C(A)$, on C denota la complexitat.

En el cas més habitual, quan parlem de complexitat ens referim a la *complexitat temporal* i analitzem el nombre de comparacions, iteracions, assignacions, etc.

Normalment, es dóna la complexitat en el *pitjor cas*, així tenim una fita superior. És evident que la complexitat del cas més favorable no és interessant. Sí que és interessant la complexitat en el cas mitjà, però aquesta pot resultar difícil de calcular i, igualment, no ens dóna una fita superior.

Definició 8.

Una funció (pròpia) de complexitat és una funció natural de variable natural $f : \mathbb{N} \rightarrow \mathbb{N}$ monòtona creixent ($f(n+1) \geq f(n)$, $\forall n \in \mathbb{N}$).

Definició 9.

Donades dues funcions de complexitat f i g , direm que f és de l'ordre de g , escrit $f = O(g)$ o $f(n) = O(g(n))$, si existeix un real positiu c i un natural n_0 tals que $f(n) \leq cg(n)$, $\forall n \geq n_0$. Direm que f i g tenen la mateixa raó de creixement si $f = O(g)$ i $g = O(f)$.

Exemple 18.

Siguin $f(n) = 5n^3 + 2n^2 + n$ i $g(n) = n^3$. Clarament $g = O(f)$, però resulta que a l'inrevés també és veritat:

$$f(n) \leq 5n^3 + 2n^3 + n^3 = 8n^3 \leq 8g(n).$$

Per tant, $f = O(g)$ i tenim que f i g tenen la mateixa raó de creixement.

En el cas de polinomis –que és molt habitual–, només importa el grau del polinomi. No se sol dir que un algorisme tingui una complexitat $C = 2n^4 + n^2$, sinó que té una complexitat $C = O(n^4)$.

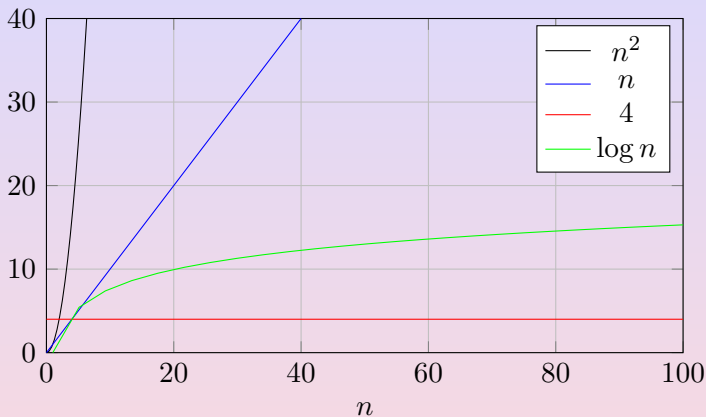
El que és important és com creix la complexitat, de quin tipus és la nostra funció de complexitat. Una diferència molt important és quan aquest creixement és polinòmic, o bé és superior.

Definició 10.

Una funció de complexitat f està fitada polinòmicament si existeix $r \in \mathbb{N}$ tal que $f(n) = O(n^r)$. En canvi, una funció d'ordre b^n ($b > 1$), n^n o $n!$ es diu que creix exponencialment.

La **taxa de creixement** de la funció de cost o complexitat és el terme de la funció que creix més ràpidament a mesura que augmenta la mida, n , del problema. La taxa de creixement dóna l'ordre de magnitud de la complexitat d'un problema.

La figura següent ens mostra el comportament d'algunes taxes de creixement associades a funcions de complexitat. Podem destacar com, a mesura que n augmenta, les gràfiques se separen i la diferència entre aquestes es fa més gran. Així, podem dir que la funció $\frac{1}{2}(n^2 - n)$ té la *taxa de creixement* més gran (n^2). A continuació ve la funció $4n + 4$, després la funció $\lfloor \log_2 n \rfloor$ i, finalment, la funció constant 4 que correspon a la funció que té la taxa de creixement més petita.



Taxes de creixement.

Funcions de complexitat

La taula de la figura següent mostra numèricament diverses taxes de creixement. Observeu que per a valors petits de n les diferències són relativament petites, però, a mesura que n augmenta, les diferències es fan grans. En particular, la columna de 2^n és la que representa la taxa de creixement més gran.

$\log n$	n	n^2	2^n
0	1	1	2
1	2	4	4
2.3	5	25	32
3.3	10	100	1024
3.9	15	225	32768
4.3	20	400	1048576
5.6	50	2500	1125899906842620
6.6	100	10000	12676506002282300000000000000000

Taxes numèriques de creixement.

La idea és que una complexitat polinòmica correspon a algorismes *eficients*. Els problemes que es poden resoldre amb algorismes eficients sovint s'anomenen *tractables*. Els que tenen complexitat superior a la polinòmica (per exemple, exponencial) s'anomenen *intractables*.

Naturalment pot semblar contradictori considerar eficient un algorisme de complexitat $O(n^{1000})$, però resulta que:

- Aquestes complexitats no es donen a la pràctica. Les complexitats polinòmiques solen ser de l'ordre de n , n^2 , n^3 , n^4 , però molt poques vegades són de grau superior.
- Qualsevol funció de creixement exponencial acabaria sent superior igualment.

Resumint, podem dir, de manera intuïtiva, que:

- problema tractable $\approx$ algorisme eficient $\approx$ complexitat polinòmica $\approx$ “fàcil”
- problema intractable $\approx$ algorisme ineficient $\approx$ complexitat no polinòmica $\approx$ “difícil”

En el darrer capítol, formalitzarem i estudiarem més en profunditat aquests conceptes.