

## Aproximació no lineal i mostratge comprimit

JOAQUIM BRUNA

**Resum:** En aquest article donem una pinzellada a un camp relativament nou de la matemàtica, el *mostratge comprimit*, un terme que correspon a l'expressió *compressed sensing* o *compressive sampling*. És una branca del tractament del senyal que d'alguna manera ha aparegut de forma natural associada a un altre gran camp ben modern i present, l'anomenat *big data analysis*. El mostratge compressiu no tracta pas de la manipulació de grans bases de dades per extreure'n informació útil, sinó justament de no generar informació inútil, innecessària. Per a l'exposició, ens referirem breument a una altra teoria que té entitat per si sola, la *teoria de l'aproximació no lineal*.

**Paraules clau:** discretització, aproximació lineal, aproximació no lineal, bases hilbertianes, mostratge comprimit, vectors rars, descodificadors, matrius aleatòries, bases incoherents.

**Classificació MSC2010:** 94A12, 68P30, 41A46.

### 1 Analògic vs. digital

Les matemàtiques sovint utilitzen en els seus models per descriure el món funcions analògiques  $f(t)$ ,  $f(x)$ ,  $t, x \in I$ , on  $I$  designa aquí un interval, acotat o no. Els models teòrics suposen que  $x$  o  $t$  és una variable independent que pot prendre tots els valors de  $I$ , un continu de valors, i podem veure  $f$  com un vector que té un continu de components. Com que les matemàtiques pretenen quantificar magnituds, se suposa en els models que aquestes funcions són quantificables en algun sentit. El més comú és imposar que tenen energia finita,

$$\|f\| = \left( \int_I |f(x)|^2 dx \right)^{\frac{1}{2}} < \infty$$

i hom diu llavors que  $f \in L^2(I)$ . Hem de veure aquesta expressió com la versió contínua de la norma euclidiana que ens és familiar, ja que no fem altra cosa

---

Aquest article és una versió desenvolupada de la lliçó inaugural de Matemàtiques del curs 2013–2014 a la Universitat Autònoma de Barcelona, i es nodreix de les referències [7], [8] i [10].

que sumar el quadrat de totes les components (infinites) del vector  $f$ . Així,  $L^2(I)$  és l'espai euclidià d'un continu de dimensions, i la norma ens serveix per quantificar com són de properes dues funcions,

$$\|f - g\| = \left( \int_I |f(x) - g(x)|^2 dx \right)^{\frac{1}{2}}.$$

Quan parlem d'una *digitalització o discretització* de  $f$ , ens referim d'una forma imprecisa a quelcom que representa o aproxima  $f$  però que no depèn d'un continu de dimensions, sinó d'un nombre finit o, com a molt, numerable de dimensions. Sovint això es formula per a funcions d'un determinat subespai  $E$  de  $L^2(I)$ . Per precisar, aquí direm que una digitalització (ideal) de  $f \in E \subset L^2(I)$  consisteix senzillament a expressar el vector  $f$  en una base ortonormal numerable (base hilbertiana)  $(\psi_n)$  de  $E$ . Això és

$$f = \sum_n \langle f, \psi_n \rangle \psi_n,$$

on els coeficients són les correlacions

$$\langle f, \psi_n \rangle = \int_I f(x) \overline{\psi_n(x)} dx.$$

Les correlacions  $\langle f, \psi_n \rangle$  constitueixen una *digitalització* de  $f$ .

El concepte de *base ortonormal* és, per tant, el mateix que el de *base cartesiana de l'espai euclidià*. Els vectors  $\psi_n$  són unitaris i perpendiculars dos a dos,  $\langle \psi_n, \psi_m \rangle = 0$ , si  $n \neq m$ , i hom té el teorema de Pitàgores

$$\|f\|^2 = \sum_n |\langle f, \psi_n \rangle|^2,$$

que en aquest context s'anomena *teorema de Parseval*.

L'exemple històricament més important és la base de Fourier de sinus i cosinus o, si es vol, d'exponencials complexes. Si  $I = [-a, a]$  és un interval acotat, la base de Fourier de  $L^2(I)$  consisteix en les exponencials complexes

$$\frac{1}{\sqrt{2a}} e^{\frac{\pi}{a} int}, \quad n \in \mathbb{Z}.$$

El desenvolupament en sèrie de Fourier pren la forma

$$f(t) = \sum_n c_n e^{\frac{\pi}{a} int},$$

amb coeficients

$$c_n = \frac{1}{2a} \int_{-a}^a f(t) e^{-\frac{\pi}{a} int},$$

que s'anomenen *coeficients de Fourier*. Evidentment, tota funció  $f \in L^2(I)$  s'identifica amb una funció  $2a$ -periòdica, de manera que el desenvolupament anterior ve a dir que tota funció  $2a$ -periòdica és una superposició, és a dir, una suma, de les funcions  $2a$ -periòdiques més elementals, que són  $\cos(\frac{\pi}{a} nt)$ ,  $\sin(\frac{\pi}{a} nt)$ ,  $n \in \mathbb{N}$ .

Un altre exemple paradigmàtic és el conegut teorema de Shannon-Whittaker-Kotelnikov. Sigui  $E$  la classe de funcions  $f \in L^2(\mathbb{R})$  que s'obtenen com a superposició de sinus i cosinus de freqüències  $\omega$ , amb  $\omega \leq a$ ,

$$f(x) = \int_{|\omega| \leq a} g(\omega) e^{2\pi i \omega x} d\omega, \quad \text{amb } g \in L^2(\mathbb{R}).$$

Aquestes són les funcions de *banda limitada*, amb amplada de banda  $a$ . Llavors

$$f(x) = \sum_n f\left(\frac{n}{2a}\right) \psi_n(x), \quad \text{on } \psi_n(x) = \frac{\sin \pi(2ax - n)}{\pi(2ax - n)}.$$

Les funcions  $\psi_n$ , que són traslladades i reescalades de la funció sinus cardinal  $\frac{\sin \pi x}{\pi x}$ , formen una base ortonormal de  $E$ ; en aquest cas, les correlacions  $\langle f, \psi_n \rangle$  coincideixen amb els valors  $f\left(\frac{n}{2a}\right)$  i  $\frac{1}{2a}$  s'anomena *el pas de Nyquist*. Matemàticament, aquest resultat és equivalent al que hem comentat, en el sentit que tota funció de  $L^2(I)$  es pot escriure com la suma d'una sèrie de Fourier.

Si, a més,  $f$  tingui suport en  $[-T, T]$ , això significaria que depèn d'aproximadament  $4Ta$  paràmetres. Llevat del cas que  $f = 0$ , no hi ha funcions de banda limitada amb suport compacte, perquè tota funció de banda limitada té una extensió entera; tanmateix, el treball de Landau i Pollack mostra que l'espai dels senyals que aproximadament tenen suport temporal de mida  $T$  i aproximadament amplada de banda  $a$  té dimensió aproximadament  $4Ta$ , on, és clar, cal precisar el significat en cada cas del terme *aproximadament*.

Un altre exemple molt important de bases i de digitalització són les *bases d'ondetes*. Ens limitarem aquí a un cas especial. Una *ondeta amb suport compacte* és una funció  $\psi$  amb suport compacte dins l'interval  $(-1/2, 1/2)$ , normalitzada, amb la meravellosa propietat que les versions reescalades i dilatades

$$\psi_{k,m}(x) = 2^{\frac{k}{2}} \psi(2^k x - m), \quad k, m \in \mathbb{Z}$$

formen una base hilbertiana de  $L^2(\mathbb{R})$ , és a dir,

$$f = \sum_{k,m} \langle f, \psi_{k,m} \rangle \psi_{k,m}, \quad \text{per a } f \in L^2(\mathbb{R}).$$

Aquí hi ha un doble índex  $(k, m)$  i les correlacions  $\langle f, \psi_{k,m} \rangle$  són mitjanes ponderades de  $f$  en l'interval diàdic de mida  $2^{-k}$  centrat en  $\frac{m}{2^k}$ .

Veiem que en les ondetes hi ha dos paràmetres, un paràmetre de posició  $m$  i un paràmetre d'escala  $k$ . L'exemple més senzill és l'ondeta de Haar, que és la funció que val  $-1$  en  $[-\frac{1}{2}, 0]$  i  $1$  en  $[0, \frac{1}{2}]$ . L'existència d'ondetes d'aquest tipus, que, a més, són regulars, és un fet molt important, degut a Daubechies.

Un tercer exemple ben clàssic de bases el donen les diverses famílies de polinomis  $(p_n)$ ,  $p_n$  de grau  $n$ , que formen una base hilbertiana de  $L^2(0, 1)$ , o de  $L^2(0, 1)$  amb un pes. Exemples en són els polinomis de Hermite, Laguerre, Jacobi, Gegenbauer, Chebyshev, Legendre, etc. Cada problema de Sturm-Liouville porta de forma natural a una base d'aquestes característiques.

## 2 Aproximació lineal i no lineal

Suposem que volem aproximar  $f$  amb una informació de mida  $N$  utilitzant una base  $(\psi_n)$

$$f = \sum_n c_n \psi_n.$$

Una forma de fer-ho és, senzillament, mitjançant els  $N$  primers coeficients

$$f^N = \sum_{n=1}^N c_n \psi_n, \quad \|f - f^N\| = \left( \sum_{n>N} |c_n|^2 \right)^{\frac{1}{2}} \rightarrow 0, \quad N \rightarrow \infty.$$

Notem que aquesta definició pressuposa que la base  $(\psi_n)$  està ordenada o jerarquizada d'alguna forma. Per exemple, en termes de la freqüència en la base de Fourier, la grandària dels paràmetres de posició i freqüència, etc. Òbviament, en aquest cas, hom té  $(f + g)^N = f^N + g^N$ , és a dir, l'aproximació és lineal.

Ara bé, això no és el millor que podem fer. Si prenem els coeficients  $c_n$  que corresponen a un subconjunt  $A$  dels números naturals i formem

$$f^A = \sum_{n \in A} c_n \psi_n,$$

tindrem

$$\|f - f^A\| = \left( \sum_{n \notin A} |c_n|^2 \right)^{\frac{1}{2}}$$

i, per tant, la millor aproximació de  $f$  utilitzant  $N$  coeficients l'obtidrem ordenant de més gran a més petit en valor absolut els coeficients  $c_n$  (que tendeixen a zero quan  $n \rightarrow \infty$ ) i quedant-nos amb els  $N$  coeficients més grans, els més significatius. Així, definim

$$f_N = \sum_{k=1}^N c_{n_k} \psi_{n_k}, \quad |c_{n_1}| \geq |c_{n_2}| \geq |c_{n_3}| \dots$$

Aquesta és ara una aproximació adaptativa però no lineal:  $(f + g)_N \neq f_N + g_N$ .

És natural preguntar-se com són de bones aquestes aproximacions. Quantitativament: com de gran hem de prendre  $N$  per tal que l'error sigui més petit que una quantitat  $\varepsilon$  prefixada? Aquesta qüestió s'estudia de la manera següent: si  $E$  és una determinada classe de funcions, com decau  $\|f - f_N\|$  si  $f \in E$ ? Típicament, voldríem, per exemple, que fos

$$\|f - f_N\| \leq C \|f\| \frac{1}{N^\alpha},$$

amb un valor de  $\alpha$  com més gran millor. Aquest exponent  $\alpha$  depèn de la classe  $E$  i de la base utilitzada  $(\psi_n)$ .

Les bases d'ondetes són molt importants en les aplicacions. El fet matemàtic que ho explica és que, per a moltes classes  $E$  de funcions (particularment, les que modelitzen imatges), les bases d'ondetes donen el millor exponent  $\alpha$ , de manera que, amb  $N$  no gaire gran, l'aproximació de  $f$  per  $f_N$  ja és prou bona. Dit d'una altra manera, les bases d'ondetes tenen la propietat de representar acuradament funcions d'interès pràctic amb molt pocs coeficients significatius, perquè la seva expressió exacta té una expressió rara, *sparse*, amb molts coeficients molt petits, en les bases d'ondetes. Això les fa especialment útils, per exemple, a l'hora de comprimir imatges en les nostres càmeres digitals. En termes generals, si una imatge es representa en una base d'ondetes de Daubechies (més precisament, en la seva versió bidimensional), hi ha aproximadament  $10^6$  coeficients; si ens quedem amb el cinc per cent dels coeficients més significatius, fent zero els altres, i fem la reconstrucció a partir d'aquests coeficients, veurem una imatge pràcticament idèntica.

### 3 Un nou pas: el mostratge comprimit (*compressed sensing o compressive sampling*)

En la secció anterior, hem vist la utilitat de l'aproximació no lineal en bases d'ondetes. Representades en bases d'ondetes, moltes funcions d'interès pràctic s'aproximen acuradament de forma no lineal.

Però reflexionem una mica. Hom fa l'esforç d'obtenir un milió de coeficients per després negligir-los pràcticament tots. No és gens eficient això!

És en aquest punt on apareix la pregunta natural, clau, i que ens portarà a un nou paradigma, el del *mostratge comprimit*: és possible dissenyar algun algorisme que ens permeti obtenir directament  $f_N$  només amb (aproximadament)  $N$  observacions?

La resposta, sorprenent, és sí, i la dona la teoria del mostratge comprimit. L'objectiu d'aquesta secció és explicar en quin sentit això és cert i, sobretot, de quina manera. Veurem com, en la resposta a aquesta pregunta, es combinen nocions d'àlgebra lineal —potser no exactament de l'àlgebra lineal estàndard— amb nocions estocàstiques molt actuals, com ara les matrius aleatòries.

Començarem formulant el problema en el marc de l'àlgebra lineal.

Tenim un vector  $f \in \mathbb{R}^D$ , on  $D$  és enorme, per exemple, el nombre de píxels d'una imatge. Podem pensar també que  $f$  és una funció definida a  $\{1, 2, \dots, D\}$ . Tenim una expressió de  $f$  en una base ortonormal

$$f = \sum_n x_n \psi_n, \quad f = \Psi X, \quad \text{on } \Psi = (\psi_1, \dots, \psi_D) \text{ i } X = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_D \end{pmatrix}.$$

Suposem que  $f$  és  $N$ -rar en la base  $\Psi$ , és a dir, que  $f = f_N$  (que vol dir que  $f$  tan sols té  $N$  coeficients no nuls), o bé que és *compressible*, en el sentit

que  $\|f - f_N\| = \|X - X_N\|$  tendeix a zero molt ràpidament. Una observació fonamental a tenir en compte per entendre la situació és la següent: sabem que  $f$  és  $N$ -rar en la base de les  $\psi_n$  (per exemple, perquè  $f$  és una imatge i la base és una base d'ondetes), però no sabem quins són els  $N$ -coeficients no nuls (si ho sabéssim, la situació fóra trivial, la resoldríem amb l'àlgebra lineal estàndard).

Modelitzem ara el mostreig de  $f$ , la informació que en tenim, mitjançant unes correlacions amb altres funcions  $\phi_k$  linealment independents:

$$y_k = \langle f, \phi_k \rangle, \quad k = 1, \dots, M,$$

on el nombre de mostres és  $M$ , que hem de pensar com un nombre molt més petit que  $D$ . Llavors la pregunta és: podem recuperar  $f$  a partir dels  $y_k$ ? Com que  $f = f_N$ , si  $f$  és  $N$ -rar, depèn de  $N$  coeficients, el millor que podem esperar és que  $M = N$ .

## 4 L'àlgebra lineal dels vectors rars

Representem-ho tot en termes matricials

$$Y = \Phi f = \Phi \Psi X = AX, \quad \text{on } A: \mathbb{R}^D \rightarrow \mathbb{R}^M \text{ i } M \ll D.$$

La matriu  $A = \Phi \Psi$ , d'ordre  $M \times D$ , s'anomena *de mostratge* (*sensing matrix*), i té rang  $M$ . Llavors pretenem recuperar  $X$  de  $Y = AX$  sabent que  $X$  és  $N$ -rar o bé compressible. Posem  $\Sigma_N$  per designar la classe dels vectors  $N$ -rars de  $\mathbb{R}^D$ . Tenim moltes menys equacions,  $M$ , que incògnites,  $D$ , però sabem que només  $N$  incògnites no són zero, sense saber, però, quines.

En general, un *descodificador* és una aplicació

$$\Delta: \mathbb{R}^M \rightarrow \mathbb{R}^D$$

tal que  $\Delta AX = X$  si  $X \in \Sigma_N$ . Un descodificador tria per a cada  $Y \in \mathbb{R}^M$  un vector  $\Delta(Y)$  de la varietat lineal  $B(Y) = \{Z : AZ = Y\}$ .

Un descodificador no és necessàriament lineal, si bé aquí suposarem per simplificar que  $\Delta 0 = 0$ . Es vol, per tant, que un descodificador sigui un invers per l'esquerra de  $A$  sobre els vectors rars. Per definició, són inversos per la dreta de  $A$ ,  $A\Delta Y = Y$ . Notem que triant en  $B(Y)$  el vector  $Z$  de norma mínima s'obté un invers per la dreta, lineal, que pren valors en l'ortogonal del nucli de  $A$ .

Volem que  $AX$  determini  $X$  per a  $X \in \Sigma_N$ , és a dir:  $X, X' \in \Sigma_N$ , amb  $AX = AX'$  ha d'implicar  $X = X'$ , o bé, si  $X - X' \in \ker(A)$ , llavors  $X = X'$ . Volem, per tant, que  $\ker(A) \cap \Sigma_{2N} = 0$ . De fet, en aquest cas, podem definir un descodificador. Definim senzillament  $\Delta(Y)$  triant entre tots els vectors  $Z$  tals que  $AZ = Y$  un que tingui suport mínim, és a dir, amb el màxim nombre de components nul·les. Llavors, si  $X$  és  $N$ -rar,  $\Delta AX$  és un vector  $Z$  tal que  $AZ = AX$  que té suport mínim, i, per tant, també és  $N$ -rar. En conseqüència,  $X - Z \in \ker(A) \cap \Sigma_{2N}$  i  $Z = X$ .

DEFINICIÓ 1. Associem a cada matriu  $A$  d'ordre  $M \times D$  el número  $s(A)$  definit com el més petit nombre de columnes de  $A$  que són linealment dependents. És a dir, qualssevol  $s(A) - 1$  columnes de  $A$  són sempre linealment independents.

A diferència de la noció de *rang habitual*, el número  $s(A)$  depèn de  $A$  i no només del subespai engendrat per les columnes de  $A$ . Evidentment, hom té que  $s(A) \leq \text{rang}(A) + 1$ .

La igualtat  $\ker(A) \cap \Sigma_{2N} = 0$  significa que no poden haver-hi mai  $2N$  columnes linealment dependents, és a dir, que qualssevol  $2N$  columnes de  $A$  han de ser linealment independents, això és,  $2N \leq s(A) - 1$ . Així, hom té que  $Y = AX$  determina  $X \in \Sigma_N$ , si i només si  $s(A) > 2N$ . Ens interessen, doncs, matrius que compleixin aquesta condició, que, tal com hem vist, és equivalent a l'existència d'un descodificador  $\Delta$  que recuperi  $X \in \Sigma_N$  de  $Y = AX$ .

Naturalment, aquesta condició implica que  $2N \leq \text{rang}(A)$  i, per tant, que  $2N \leq M$ . Fixats  $N, D, M$  amb  $M \geq 2N$ , sempre hi ha matrius d'ordre  $M \times D$  tals que qualssevol  $2N$  columnes siguin linealment independents. És suficient trobar  $D$  vectors a  $\mathbb{R}^{2N}$  tals que qualssevol  $2N$  d'ells siguin linealment independents. Si  $0 < t_1 < t_2 < \dots < t_D$  són arbitraris, la matriu que té entrada  $t_j^{i-1}$  a la fila  $i$ , columna  $j$ , té tots els menors d'ordre  $2N \times 2N$  que són matrius de Vandermonde i, per tant, invertibles. Aquestes matrius són, però, mal condicionades i, per tant, no adequades per al càlcul numèric.

Ara bé, per tal que un descodificador  $\Delta$  tingui interès pràctic, ha de ser robust, en el sentit que si  $X \notin \Sigma_N$  però  $\|X - X_N\|$  és petit, voldríem que també  $\Delta AX$  fos proper a  $X$  d'una forma controlada. El més natural és imposar que existeixi una constant  $C > 0$  tal que

$$\|\Delta AX - X\| \leq C\|X - X_N\|, \quad (1)$$

que, naturalment, quantifica el fet que  $\Delta AX = X$ , si  $X$  és  $N$ -rar.

Òbviament, això implica

$$\|X\| \leq C\|X - X_N\|, \quad X \in \ker(A),$$

per a una certa constant  $C$ . De fet, implica aquesta mateixa desigualtat, però amb  $2N$  en lloc de  $N$  (vegeu [8]):

$$\|X\| \leq C\|X - X_{2N}\|, \quad X \in \ker(A). \quad (2)$$

En efecte: donat  $X \in \ker(A)$ , considerem una descomposició de  $X_{2N}$  en dos vectors  $N$ -rars,  $X_{2N} = X_1 + X_2$ , i sigui  $X_3 = X - X_{2N}$ . Com que  $-X_1 \in \Sigma_N$ , tindrem que  $-X_1 = \Delta A(-X_1)$ ; com que  $X \in \ker(A)$ , tindrem que  $A(-X_1) = A(X_2 + X_3)$ ; per tant,  $-X_1 = \Delta A(X_2 + X_3)$ . Aleshores, per (1),

$$\|X\| = \|X_2 + X_3 - \Delta A(X_2 + X_3)\| \leq C\|(X_2 + X_3) - (X_2 + X_3)_N\|.$$

Ara bé, com que  $X_2$  és  $N$ -rar, és clar que la darrera expressió és menor o igual que  $\|X_3\| = \|X - X_{2N}\|$ .

Quan es compleix (2), hom diu que  $A$  té la propietat NSP (null space property) d'ordre  $2N$  respecte de la norma euclidiana.

A la pràctica, els descodificadors han de ser també robusts respecte dels errors, perquè les mostres poden contenir soroll. No mesurarem  $Y = AX$  exactament, sinó

$$Y = AX + Z,$$

on  $Z$  és un error, estocàstic o determinista. Si  $\Delta$  és un descodificador, diem que és *robust* si

$$\|\Delta(AX + Z) - X\| \leq C\|Z\|, \quad X \in \Sigma_N, \quad Z \in \mathbb{R}^D. \quad (3)$$

Anàlogament a les altres propietats, aquesta condició natural —l'existència d'un descodificador robust— implica una propietat de la matriu  $A$ , concretament

$$\|A(X)\| \geq \frac{1}{C}\|X\|, \quad X \in \Sigma_{2N}. \quad (4)$$

Per veure-ho, siguin  $X, Y \in \Sigma_N$  i definim  $Z = \frac{1}{2}A(X - Y)$ , de manera que

$$AX - Z = AY + Z = \frac{1}{2}A(X + Y).$$

Si  $W = \Delta(AX - Z) = \Delta(AY + Z)$ , (3) implica

$$\|X - Y\| \leq \|X - W\| + \|W - Y\| \leq 2C\|Z\| = C\|AX - AY\|.$$

Fixem-nos que (4) implica que  $X \in \Sigma_N$  es pot recuperar de  $AX$ .

La definició següent fou introduïda a [6] i [2].

**DEFINICIÓ 2.** La matriu  $A$  satisfà la propietat RIP (*restricted isometry property*) d'ordre  $N$ , si hi ha  $\delta_N$  petit tal que

$$(1 - \delta_N)\|X\|^2 \leq \|AX\|^2 \leq (1 + \delta_N)\|X\|^2, \quad X \in \Sigma_N.$$

Significa que qualssevol  $N$  columnes de  $A$  són gairebé ortogonals. Per tant, si  $A$  satisfà la propietat RIP d'ordre  $2N$ ,  $A$  preserva aproximadament la distància entre dos vectors  $N$ -rars.

La propietat RIP implica una versió de la propietat NSP, però amb la norma  $L^1$ . La norma  $L^1$  d'un vector  $X$  es defineix com a

$$\|X\|_1 = \sum_{i=1}^D |x_i|.$$

Per a un vector  $X \in \Sigma_N$ , la desigualtat de Schwarz implica que

$$\|X\|_1 \leq \sqrt{N}\|X\|.$$



El resultat precís, que no demostrarem, és que si  $A$  té la propietat RIP d'ordre  $N$  amb una constant  $\delta_N < \sqrt{2} - 1$ , llavors

$$\|X\| \leq C \frac{\|X - X_{2N}\|_1}{\sqrt{N}}, \quad X \in \ker(A),$$

amb  $C = \frac{2}{1 - (1 + \sqrt{2})\delta_N}$ .

## 5 El descodificador basat en la norma $L^1$

Reprenem la situació anterior. Tenim  $Y = AX$ , on  $A$  és una matriu de mostratge  $M \times D$  amb  $M \ll D$ . Tanmateix, pretenem recuperar  $X \in \mathbb{R}^D$  de  $Y = AX \in \mathbb{R}^M$  utilitzant la informació que  $X$  és  $N$ -rar o  $N$ -compressible. A la secció anterior, hem vist condicions sobre la matriu  $A$  que són necessàries per tal que pugui existir un descodificador  $\Delta$  que permeti obtenir  $X$  de  $AX$  quan  $X \in \Sigma_N$  d'una forma estable i robusta. En aquesta secció, descriurem la situació pel que fa a la suficiència d'aquestes condicions, és a dir, a la construcció de descodificadors concrets. Recordem que definir un descodificador vol dir simplement definir un criteri per tal de seleccionar per a cada  $Y$  un vector de la varietat lineal  $B(Y)$ .

Atès que el nostre propòsit principal és recuperar vectors rars, el més natural, allò que sembla més intuïtiu, és triar el més rar dels vectors de  $B(Y)$ , és a dir, podem considerar el descodificador  $\Delta_0(Y) = Z$ , on  $Z$  és el vector  $Z \in B(Y)$  que minimitzi el nombre  $\|Z\|_0$  de components no nul·les. Si la matriu  $A$  és injectiva sobre els vectors  $N$ -rars, és a dir,  $s(A) > 2N$ , ja hem vist que  $\Delta AX = X$ , si  $X \in \Sigma_N$ . Ara bé, el problema amb aquest descodificador és que  $\|Z\|_0$  no és convex i la implementació pràctica no és factible. De fet, s'ha demostrat que implementar  $\Delta_0$  en un ordinador és *NP-hard*, és a dir, d'una gran complexitat de càlcul.

Hem vist que la propietat NSP d'ordre  $2N$ , equivalent a l'equació (2), és necessària per a l'existència d'un descodificador que compleixi (1). Ara veurem que també és suficient; vegeu [8]. En efecte, en aquest cas, triem entre tots els vectors  $Z$  tals que  $AZ = Y$  aquell per al qual  $\|Z - Z_N\|$  és mínim, és a dir, el que millor s'aproxima per vectors  $N$ -rars.

Com que  $X - Z$  està en el nucli d' $A$ , (2) implica

$$\|X - Z\| \leq C \|X - Z - (X - Z)_{2N}\|.$$

En aquest punt, recordem que  $X_{2N}$  és la millor aproximació de  $X$  amb  $2N$  coeficients; per tant, hom té, en general,  $\|(U+V) - (U+V)_{2N}\| \leq \|U - U_N\| + \|V - V_N\|$ . Amb això, l'expressió anterior és menor o igual que

$$C(\|X - X_N\| + \|Z - Z_N\|).$$

Per definició,  $\|Z - Z_N\| \leq \|X - X_N\|$  i, per tant,

$$\|X - Z\| \leq 2C \|X - X_N\|.$$

Així, hem vist que la propietat NSP d'ordre  $2N$  és equivalent a l'existència d'un descodificador  $\Delta$  que compleixi (1). Com que  $X_N$  és, per definició, la millor aproximació de  $X$  amb  $N$  coeficients, la propietat NSP d'ordre  $2N$  és equivalent a la condició

$$\|X\| \leq C\|X - X_\Gamma\|, \quad X \in \text{Ker}(A), \quad \text{cardinal}(\Gamma) \leq N. \quad (5)$$

Aquí  $\Gamma \subset \{1, 2, \dots, N\}$  i el vector  $X_\Gamma$  és el que s'obté de  $X$  conservant les components que corresponen a  $\Gamma$  i fent zero les altres.

Ara bé, veurem tot seguit que això implica que  $M \geq C^{-2}D$  (c.f. [8]). Per al cas que el cardinal de  $\Gamma$  sigui 1, (5) significa que per a tot  $j = 1, \dots, D$  hom té

$$\sum_{i=1}^D x_i^2 \leq C^2 \sum_{i \neq j} x_i^2,$$

que implica

$$x_j^2 \leq (C^2 - 1) \sum_{i \neq j} x_i^2 = (C^2 - 1)(\|X\|^2 - x_j^2),$$

i, per tant,

$$x_j^2 \leq \left(1 - \frac{1}{C^2}\right) \|X\|^2.$$

Això hauria de ser cert per a tot  $X$  en el nucli de  $A$ . Sigui  $e_1, \dots, e_D$  la base canònica de  $\mathbb{R}^D$  i sigui  $v_1, \dots, v_{D-M}$  una base ortonormal del nucli de  $A$ . Sigui  $P$  la projecció ortogonal sobre el nucli de  $A$ . Llavors, per a  $X = P(e_j)$  obtenim

$$\langle P(e_j), e_j \rangle^2 \leq \left(1 - \frac{1}{C^2}\right),$$

que és el mateix que

$$\sum_{i=1}^{D-M} \langle e_j, v_i \rangle^2 \leq \left(1 - \frac{1}{C^2}\right), \quad j = 1, \dots, D.$$

Sumant respecte de  $j$  obtenim

$$D - M = \sum_{i=1}^{D-M} \|v_i\|^2 \leq D \left(1 - \frac{1}{C^2}\right),$$

és a dir,  $M \geq C^{-2}D$ .

Aquest és un resultat *negatiu*, ja que ens indica que  $M$  ha de ser de l'ordre de  $D$  i no de  $N$ , que és el que esperàvem.

Una tercera possibilitat és minimitzar una norma diferent de l'euclidiana: per exemple, la norma  $L^1$ . Aquesta norma, en un cert sentit, està més ben adaptada a la raresa dels vectors. Genèricament, el vector d'una varietat lineal que minimitza la norma  $L^1$  tendeix a ser rar, com es veu a la figura 1.

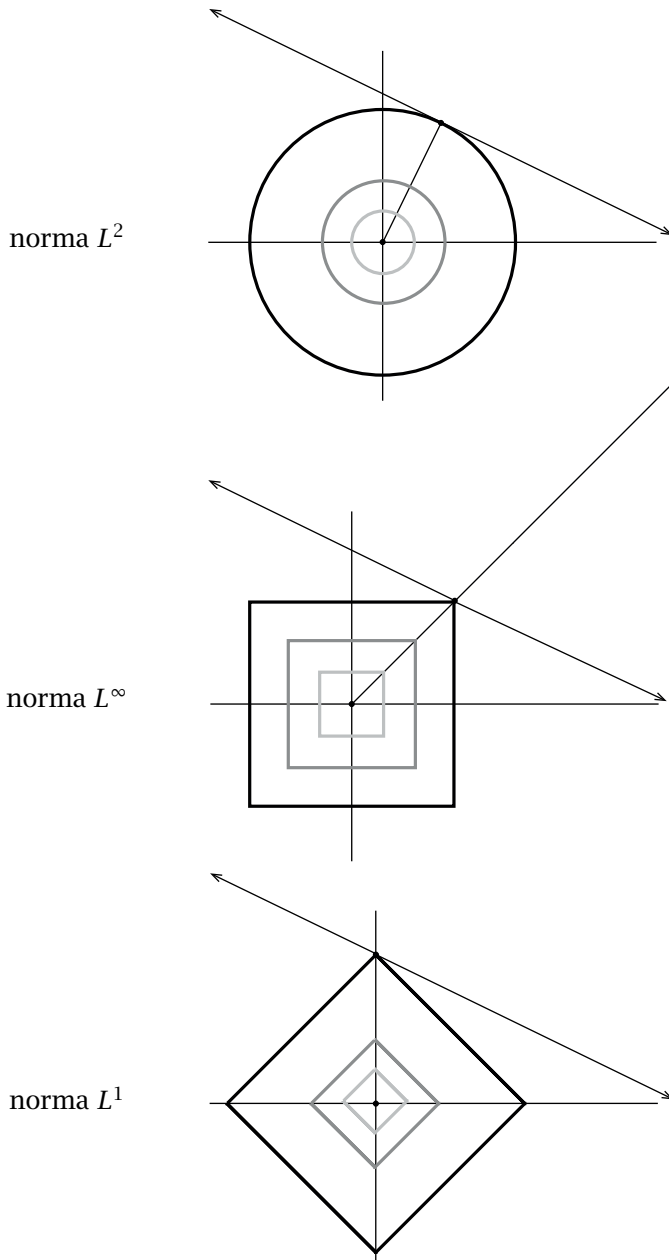


FIGURA 1: Els gràfics mostren la selecció, en una varietat lineal (en aquest cas una recta), del vector que minimitza una certa norma. Equivalentment, mostren com una bola associada a la norma va creixent fins que toca a la varietat lineal. Observi's que tan sols per a la norma  $L^1$  el punt de contacte és un vector rar (en els eixos de coordenades).

En conseqüència, sembla raonable fer la recuperació dels vectors rars minimitzant la norma  $L^1$ . Tornant al nostre problema, definim  $\Delta(Y)$  com el vector  $Z \in B(Y)$  que minimitzi  $\|Z\|_1$ . És a dir, per recuperar  $X$ , estudiem  $\hat{X} = \Delta AX = Z$  tal que  $AZ = AX$  minimitzi  $\|Z\|_1$ . Entre tots els vectors que són coherents amb les observacions, prenem el que minimitza la norma  $L^1$ .

Aquest és un problema de programació lineal que es pot tractar computacionalment d'una forma molt eficient.

El teorema següent confirma les expectatives.

**TEOREMA 3.** *Suposem que la matriu  $A$  compleix la propietat RIP d'ordre  $2N$  amb  $\delta_{2N} < \sqrt{2} - 1$ . Aleshores, la solució  $\hat{X}$  definida anteriorment compleix*

- $\|\hat{X} - X\| \leq C \frac{\|X - X_N\|_1}{\sqrt{N}}$ .
- $\|\hat{X} - X\|_1 \leq C \|X - X_N\|_1$ .
- $\|\hat{X} - X_N\| \leq 2C \|X - X_N\|_1$ .

*A més, aquesta reconstrucció és robusta: si donat  $\varepsilon > 0$  posem  $B(Y) = \{Z \in \mathbb{R}^D \text{ amb } \|AZ - Y\| \leq \varepsilon\}$ , la solució  $\hat{X}$  compleix*

$$\|\hat{X} - X\| \leq C \frac{\|X - X_N\|_1}{\sqrt{N}} + C\varepsilon.$$

Aquest teorema, demostrat a [5], és un resultat bastant notable. En destaquem els punts següents:

1. Si  $X$  és  $N$ -rar, aleshores  $X = X_N$  i tenim reconstrucció exacta. Si no, ens diu que la qualitat de  $\hat{X}$ , mesurada per l'error  $\|\hat{X} - X\|_1$ , és tan bona com si coneguéssim d'antuvi les  $N$  coordenades més grans de  $X$ . I, a més, és robust.
2. L'algorisme  $\Delta$  és independent de  $N$ , de les posicions dels coeficients i de les seves magnituds. Si la matriu  $A$  té la propietat RIP d'ordre  $2N$ , tindrem reconstrucció exacta.

## 6 I com trobem matrius $M \times D$ de mostratge $A$ que tinguin la propietat RIP d'ordre $N$ ?

El teorema anterior és prou satisfactori sempre que siguem capaços de trobar matrius de mostratge que compleixin la hipòtesi. De fet, ens interessa també que ho compleixin amb  $M$  —el nombre de mostres— el més petit possible, idealment de l'ordre de  $N$ . O podem pensar-ho al revés: amb  $M$  fixat, ens interessa que  $N$  sigui el més gran possible. Hi ha construccions deterministes de matrius  $A$  que compleixen la hipòtesi, però amb  $M$  massa gran. Com sovint passa, però, les construccions aleatòries gairebé sempre funcionen.

Per exemple, hom pot provar que si es prenen les entrades de  $A$  independents i idènticament distribuïdes segons una llei contínua, es complirà  $s(A) = m + 1$  amb probabilitat 1. El resultat que ens interessa és, però, el següent:

**TEOREMA 4.** *Considerem les matrius aleatòries de mida  $M \times D$  obtingudes d'alguna de les maneres següents:*

1. *Triant  $D$  vectors columna a l'atzar (amb distribució uniforme) a l'esfera unitat de  $\mathbb{R}^M$ .*
2. *Prenent com a entrades de  $A$  variables  $N(0, \frac{1}{M})$  independents.*
3. *Prenent com a entrades de  $A$  variables independents amb valors  $\pm \frac{1}{\sqrt{M}}$  de probabilitat  $\frac{1}{2}$ .*

*Llavors, si  $M \geq CN \log \frac{D}{N}$ ,  $A$  compleix la propietat RIP d'ordre  $2N$  amb constant  $< \sqrt{2} - 1$ , amb una probabilitat  $\geq 1 - e^{-cM}$ , on  $c$  és una constant que depèn de  $C$ .*

Aquest resultat no és difícil de provar: és conseqüència dels anomenats *fenòmens de concentració de mesura*; vegeu [1]. El que és significatiu en el resultat és el fet que  $M \geq CN \log \frac{D}{N}$ , és a dir, que  $M$  no és pas gaire més gran que  $N$ . Aquesta cota inferior de  $M$  és òptima en el teorema, perquè hom pot provar que tota matriu  $M \times D$  que compleixi la propietat RIP d'ordre  $2N$  amb constant  $\delta < \frac{1}{2}$  ha de satisfer l'acotació inferior anterior per a  $M$ .

En definitiva, hem vist que una estratègia efectiva és agafar matrius de mostratge aleatòries i utilitzar la minimització en norma  $L^1$ .

El cas gaussià té un valor afegit rellevant. Tornem al començament, quan la matriu de mostratge era  $A = \Phi\Psi$ . Teníem  $f = \Psi X$ , i fem un mostratge de  $f$  amb  $\Phi$ ,  $Y = \Phi f$ ,  $Y = y_1, y_2, \dots, y_M$ . Considerem  $f^* = \Psi X^*$ , on  $X^*$  és el vector de norma  $L^1$  mínima tal que

$$\langle \Psi X^*, \phi_k \rangle = y_k, \quad k = 1, \dots, M.$$

Si  $f$  és rar en la base  $\Psi$  i  $A$  compleix les hipòtesis del teorema 3, tindrem reconstrucció exacta,  $f^* = f$ . Ara bé, si  $\Phi$  és gaussiana en el sentit del teorema 4,  $A$  també és gaussiana per a tota  $\Psi$  i servirà com a matriu aleatòria.

Això significa que l'algorisme funcionarà per a totes les bases  $\Psi$ ,  $\Phi$ , és a dir, és universal. Dit d'una altra manera, no necessitem saber en quina base  $f$  és rara, només que ho és en alguna!

## 7 La coherència entre dues bases ortonormals

Hi ha altres maneres d'aproximar-se al concepte de *bona matriu de mostratge*. Una d'elles està basada en la noció de *coherència* entre dues bases. Suposarem que les funcions  $\phi_k$  amb les que prenem mostres formen part d'una base ortonormal. Dit d'una altra forma, la matriu  $\Phi$ , de mida  $M \times D$ , és una matriu obtinguda triant  $M$  files d'una matriu ortonormal  $\Gamma$ .

DEFINICIÓ 5. La coherència entre dues matrius (bases) ortonormals  $\Psi, \Gamma$  d'ordre  $D \times D$  és

$$\mu(\Psi, \Gamma) = \sqrt{D} \max_{i,j} \|\langle \gamma_i, \psi_j \rangle\|, \quad \text{on } \Gamma = (\gamma_1, \dots, \gamma_D), \Psi = (\psi_1, \dots, \psi_D).$$

Es tracta, doncs, d'una mesura del grau de correlació existent entre ambdues bases, que, per definició, és un nombre entre 1 i  $\sqrt{D}$ . El coeficient de normalització  $\sqrt{D}$  està posat en relació amb l'exemple següent, que és l'exemple principal d'un parell de bases incoherents. Prenem com a  $\Psi$  la base de Fourier,  $\psi_j(k) = D^{-\frac{1}{2}} e^{i2\pi jk/D}$ , i com a  $\Gamma$  la base canònica  $\gamma_j(k) = \delta(j - k)$ . Òbviament,  $\mu(\Psi, \Gamma) = 1$  i tenim màxima incoherència.

El teorema següent és del mateix esperit que el teorema 3 quan l'apliquem a una matriu aleatòria. Aquí,  $A$  és la matriu aleatòria  $\Phi\Psi$ , on  $\Phi$  consisteix a prendre  $M$  columnes a l'atzar de  $\Gamma$ .

TEOREMA 6 ([3]). *Suposem que  $f$  és  $N$ -rar en la base  $\Psi$ . Triem  $M$  mesures a l'atzar entre les correlacions de  $f$  respecte de la base  $\Gamma$ ,  $\langle f, \gamma_i \rangle$ . Si*

$$M \geq \mu^2(\Psi, \Gamma) N \log D,$$

*llavors la solució del problema  $f^* = \Psi X^*$ , on  $X^*$  és el vector de norma  $L^1$  mínima tal que*

$$\gamma_i = \langle \gamma_i, \Psi X^* \rangle,$$

*és exacta amb probabilitat molt propera a 1.*

El teorema ens diu que, per aconseguir minimitzar el nombre de mostres i aconseguir reconstrucció exacta amb probabilitat 1, com més incoherents siguin les bases, millor. En el cas de l'exemple de Fourier de màxima incoherència, què ens diu aquest teorema? Ens diu que si un senyal de mida  $D$  és  $N$ -rar en freqüència,

$$f(t) = \sum_{j=0}^{D-1} x_j e^{2\pi i j t / D}, \quad X \in \Sigma_N \quad (6)$$

llavors és possible reconstruir  $f$  a partir dels seus valors en  $M = N \log D$  enters presos a l'atzar entre 1 i  $D$ , i gairebé totes les tries van bé. Insistim un cop més que això funciona sense cap coneixement previ de quines són les  $N$ -freqüències actives ni les seves amplituds. Dualment, si  $f$  és  $N$ -rar a  $R^D$ , es pot recuperar  $f$  a partir de  $N \log D$  coeficients de Fourier presos a l'atzar, i gairebé totes les tries van bé. Aquest resultat, demostrat a [4], va precedir el teorema general i fou un dels primers en la teoria. És interessant contrastar-lo amb el teorema determinista següent: si  $f$  és com a (6), és possible reconstruir  $f$  exactament a partir dels seus valors en  $1, 2, \dots, 2N$  o, més generalment, en  $2N$  enters consecutius qualssevol. Aquí,  $N \log D$  és substituït per la millor cota  $2N$ , però la diferència està en el fet que, en el resultat que acabem d'esmentar, gairebé totes les tries de  $M = N \log D$  enters funcionen. També és rellevant el fet que, si hom vol que gairebé totes les  $M$  tries d'enters vagin bé, llavors cal que  $M \geq N \log D$ , és a dir, el resultat és òptim.

D'altra banda, no pot haver-hi un teorema d'aquest estil sense la component aleatòria, és a dir, de forma que la reconstrucció sigui possible per a *totes* les tries de  $M$  enters. Això és perquè hi ha senyals  $f$ ,  $N$ -rars de mida  $D$ , que tenen  $D - N$  coeficients de Fourier tots nuls.

Altres exemples de bases altament incoherents s'obtenen prenent com a  $\Psi$  les bases d'ondetes de Daubechies i com a  $\Phi$  les anomenades *bases de noiselets*; vegeu [9].

## Referències

- [1] BARANIUK, R.; DAVENPORT, M.; DEVORE, R.; WAKIN, M. «A simple proof of the restricted isometry property for random matrices». *Constr. Approx.*, 28 (3) (2008), 253-263.
- [2] CANDÈS, E. J. «The restricted isometry property and its implications for compressed sensing». *C. R. Math. Acad. Sci. Paris*, 346 (9-10) (2008), 589-592.
- [3] CANDÈS, E.; ROMBERG, J. «Sparsity and incoherence in compressive sampling». *Inverse Problems*, 23 (3) (2007), 969-985.
- [4] CANDÈS, E. J.; ROMBERG, J.; TAO, T. «Robust uncertainty principles: exact signal reconstruction from highly incomplete frequency information». *IEEE Trans. Inform. Theory*, 52 (2) (2006), 489-509.
- [5] CANDÈS, E. J.; ROMBERG, J. K.; TAO, T. «Stable signal recovery from incomplete and inaccurate measurements». *Comm. Pure Appl. Math.*, 59 (8) (2006), 1207-1223.
- [6] CANDÈS, E. J.; TAO, T. «Decoding by linear programming». *IEEE Trans. Inform. Theory*, 51 (12) (2005), 4203-4215.
- [7] CANDÈS, E. J.; WAKIN, M. B. «An introduction to compressive sampling». *Signal Processing Magazine, IEEE*, 25 (2) (2008), 21-30.
- [8] COHEN, A.; DAHMEN, W.; DEVORE, R. «Compressed sensing and best  $k$ -term approximation». *J. Amer. Math. Soc.*, 22 (1) (2009), 211-231.
- [9] COIFMAN, R.; GESHWIND, F.; MEYER, Y. «Noiselets». *Appl. Comput. Harmon. Anal.*, 10 (1) (2001), 27-44.
- [10] ELДАР, Y. C.; KUTYNIOK, G. (ed.). *Compressed sensing. Theory and applications*. Cambridge: Cambridge University Press, 2012.