Butlletí de la Societat Catalana de Matemàtiques
Vol. 34, núm. 1, 2019. Pàg. 53–89. DOI: 10.2436/20.2002.01.86

Codis detectors i correctors d'errors i algunes de les seves aplicacions a la societat de la informació

Mercè Villanueva i Cristina Fernández-Córdoba

«Maleït sigui! Si les màquines poden detectar un error, per què no podem localitzar la posició de l'error i corregir-lo?», 1947.

Richard W. Hamming (1915–1998)

Resum: En les transmissions digitals d'informació d'un emissor a un receptor a través d'un canal, normalment es produeixen errors. En aquest article s'exposen els conceptes i resultats més importants de la teoria de codis detectors i correctors d'errors, que estudia mètodes eficients per garantir una transmissió exacta de la informació. Primer es descriuen alguns exemples quotidians de codis detectors d'errors inclosos en el DNI, l'ISBN, l'IBAN i l'EAN. A continuació, es presenta la teoria clàssica dels codis correctors d'errors, que inclou els codis lineals i, dins d'aquests, els codis cíclics, que resulten més eficients a l'hora de codificar. També es descriuen les dues famílies més importants de codis cíclics, els BCH i Reed-Solomon, que permeten descodificar també de forma eficient. Finalment, es mostren dues aplicacions històriques, en les memòries d'ordinador i en la transmissió de fotografies a l'espai, i dues aplicacions més recents, en els codis QR i en l'emmagatzematge distribuït.

Paraules clau: detecció d'errors, correcció d'errors, codis lineals, codis cíclics, BCH, Reed-Solomon, aplicacions.

Classificació MSC2010: 94B05, 94B15, 11T71.

1 Introducció

Cap a l'any 1948, Claude E. Shannon va formular en els seus treballs el problema de la transmissió d'informació en termes estadístics, utilitzant models probabilístics per a les fonts d'informació i els canals de comunicació [41]. Amb aquests treballs va néixer un nou camp anomenat *teoria de la informació* [1], dins del qual es troba la teoria matemàtica de la comunicació digital, que estudia la transmissió de la informació entre un emissor i un receptor a través d'un

canal. En molts casos, els canals que es fan servir són insegurs i amb soroll, com, per exemple, en la comunicació entre dos telèfons mòbils via satèl·lit, on la informació viatja per l'espai a través d'ones.

Així, en general, la informació pot ser interceptada i manipulada per tercers. A més, es poden produir errors i interferències que alteren el senyal transmès, cosa que fa que el receptor no rebi exactament la mateixa informació que havia enviat l'emissor. Altres exemples de comunicació digital es troben en la televisió digital, l'emmagatzematge de dades en diferents dispositius (memòries, CD, Blu-ray, etc.), Internet, Internet de les coses (IoT), etc.

En la transmissió d'informació es consideren diferents mecanismes, de manera que es pugui garantir que la comunicació entre l'emissor i el receptor sigui eficient, segura i exacta. La figura 1 mostra un esquema general d'un sistema de comunicació digital a través d'un canal insegur i amb soroll. Per tal que la transmissió sigui més eficient, s'aplica un compressor que permet reduir la mida de les dades que volem enviar aprofitant la redundància que aquestes presenten. També es pot realitzar un procés de xifratge (també conegut com a *encriptació*) per tal d'evitar que un tercer pugui accedir a les dades i garantir així la seva confidencialitat i/o autenticitat. Finalment, per assegurar una comunicació fiable i exacta, es codifiquen fent servir codis correctors d'errors. És en aquesta darrera fase, estudiada dins de l'anomenada *teoria de la codificació*, en la qual ens centrarem en aquest article.

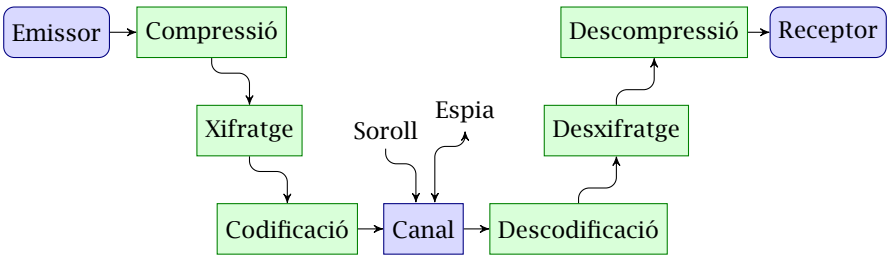

FIGURA 1: Sistema de comunicació digital.

Inicialment, la teoria de la codificació es trobava dins de l'àmbit de l'enginyeria electrònica o informàtica. A més, els canals considerats eren binaris i, per tant, els codis estudiats estaven definits sobre el cos $\mathbb{Z}_2$. A poc a poc, la teoria de la codificació s'ha anat endinsant més en l'àmbit matemàtic. Per una banda, s'ha anat dotant els codis de certa estructura algebraica que ha anat fent més eficient el procés de codificar i descodificar; i, per una altra banda, s'han considerat codis sobre alfabets diferents. Primer, es van començar a estudiar codis sobre cossos finits. A partir del 1994, arran de l'article [18], on es van estudiar codis sobre $\mathbb{Z}_4$, van començar a tenir més importància els codis sobre anells en general. També s'han considerat codis sobre alfabets mixtos (les coordenades es troben en diferents anells) [5]. Actualment, dins del camp de la teoria de la codificació, hi ha una vessant més d'enginyeria que estudia l'aplicació de mètodes de codificació i descodificació a diferents

sistemes de comunicació, i una altra vessant més matemàtica que estudia les diferents estructures algebraiques, geomètriques i combinatòries dels codis, la construcció de nous codis, l'existència de codis amb certes propietats, i la seva classificació.

Durant la transmissió de dades digitals (normalment en forma de seqüència de bits) a través de canals amb soroll, es poden produir errors i, per tant, no rebre a la sortida del canal exactament les mateixes dades que s'havien enviat. Per exemple, pot haver-hi soroll tèrmic generat per l'equipament electrònic. Els codis correctors d'errors tenen com a objectiu detectar aquests errors i corregir-los. Aquest procés permet, per exemple, rebre bones imatges des dels satèl·lits, o gaudir de la música emmagatzemada en un CD encara que el disc estigui ratllat. El preu que s'ha de pagar per corregir els errors és afegir una certa redundància a les dades que es volen transmetre.

No només en les transmissions d'informació, on el canal és un cable, l'aire o l'espai, és necessari disposar de mecanismes que puguin permetre la detecció i, si és possible, la correcció d'errors. Si considerem, per exemple, que el canal és el paper o un disc dur, ens podem plantejar si en escriure i emmagatzemar algun número llarg, volem poder detectar possibles errors. En aquests canals, els errors més freqüents són equivocar-se introduint algun dígit o bé intercanviant dos dígits. Per poder detectar aquests tipus d'errors, usualment s'afegeix redundància incorporant un nou símbol al número. Així és com s'han dissenyat codis tan quotidians com el codi del document nacional d'identitat o DNI, l'*International Standard Book Number* o ISBN dels llibres, l'*International Bank Account Number* o IBAN i el Codi de Compte Corrent o CCC dels comptes bancaris, i l'*European Article Number* o EAN, que formen part dels coneguts codis de barres, que descriurem en la secció 2.

En la secció 3, introduirem els conceptes de la teoria clàssica dels codis correctors d'errors. Primer ens centrarem en els codis lineals basats en conceptes d'àlgebra. A continuació, descriurem els codis lineals cíclics o codis cíclics que permeten codificar la informació de forma més eficient. Finalment, presentarem les dues famílies més importants de codis cíclics, els codis BCH i Reed-Solomon, que permeten també descodificar de forma eficient i que, per tant, són els que es fan servir en moltes situacions en què és necessari poder corregir errors i evitar una retransmissió de les dades.

Els primers codis lineals, els codis de Hamming, s'expliquen en la secció 4, on es veu la seva aplicació en les primeres memòries d'ordinador. En la secció 5, es descriuen els codis de Reed-Muller de primer ordre, coneguts també com a *codis de Hadamard*. A més, es mostra com alguns d'aquests codis es van utilitzar per millorar la transmissió de fotografies a l'espai. En la secció 6, ens centrarem en l'aplicació dels codis BCH i Reed-Solomon dins dels coneguts *codis QR* (*Quick Response*), que representen una evolució dels codis de barres, d'una a dues dimensions. Finalment, en la secció 7, veurem una aplicació recent dels codis correctors d'errors en el camp de l'emmagatzematge distribuït.

2 Exemples quotidians de codis detectors d'errors

En aquesta secció, descriurem alguns dels codis detectors d'errors més coneguts, ja esmentats en la introducció: el codi associat al DNI, l'ISBN dels llibres, l'IBAN i el CCC dels comptes bancaris, i l'EAN o codi de barres. Tots ells són força quotidians i ens els trobem tot sovint en el dia a dia. A més, tots estan basats en l'aritmètica modular i detecten, però no permeten, corregir els errors. A part d'aquests, n'hi ha molts més, com els que apareixen en les targetes de crèdit, els bitllets d'avió o els serveis de missatgeria, entre d'altres.

2.1 Codi DNI

El codi del document nacional d'identitat (DNI) consisteix en un número de 8 xifres decimals seguit d'una lletra. Aquesta lletra, de fet, representa la redundància que permetrà detectar els errors més freqüents en escriure el número. La lletra s'assigna segons el valor que resulta de calcular el número del DNI a $\mathbb{Z}_{23}$, o el que és el mateix, segons el residu que s'obté en dividir-lo per 23, d'acord amb les equivalències que es mostren en la taula 1.

0	1	2	3	4	5	6	7	8	9	10	11
T	R	W	A	G	M	Y	F	P	D	X	B
12	13	14	15	16	17	18	19	20	21	22	
N	J	Z	S	Q	V	H	L	C	K	E	

TAULA 1: Assignació de lletres per al DNI.

El càlcul es realitza a $\mathbb{Z}_{23}$. Es pren un número primer per tal de treballar en un cos finit. A més, s'exclouen les lletres I, O i U, perquè aquestes es poden confondre més fàcilment amb l'1, el 0 i la lletra V, respectivament. Podem simplificar els càlculs si tenim precalculades les potències de 10 a $\mathbb{Z}_{23}$. Així, com que $10^2 = 8$, $10^3 = 11$, $10^4 = 18$, $10^5 = 19$, $10^6 = 6$ i $10^7 = 14$ a $\mathbb{Z}_{23}$, calcular el número del DNI a $\mathbb{Z}_{23}$ equival a calcular $x_0 + 10x_1 + 8x_2 + 11x_3 + 18x_4 + 19x_5 + 6x_6 + 14x_7$ a $\mathbb{Z}_{23}$, on $x_7x_6x_5x_4x_3x_2x_1x_0 = \sum_{i=0}^{7} 10^i x_i$ representa el número del DNI.

EXEMPLE 1. La lletra del DNI corresponent al número 34149351 és D, ja que $34149351 = 9$ a $\mathbb{Z}_{23}$, o equivalentment, $14 \cdot 3 + 6 \cdot 4 + 19 \cdot 1 + 18 \cdot 4 + 11 \cdot 9 + 8 \cdot 3 + 10 \cdot 5 + 1 = 9$ a $\mathbb{Z}_{23}$, i la lletra corresponent al valor 9 és D d'acord amb la taula 1.

Aquest codi permet detectar si hi ha hagut un error en un dels dígits del DNI, o bé si hi ha hagut una transposició entre dos dígits [6]. En canvi, si n'hi ha dos o més, no sempre es poden detectar. També permet recuperar un dels dígits si aquest no es visualitza correctament, simplement resolent una equació lineal a $\mathbb{Z}_{23}$.

EXEMPLE 2. Continuant amb el DNI de l'exemple 1, què passa si en escriure el DNI ens equivoquem en un dígit i escrivim, per exemple, 34**2**49351D? Com

que $34249351 = 5$ a $\mathbb{Z}_{23}$ i la lletra corresponent al 5 és la M, podem detectar que hi ha hagut un error, i repassar l'escriptura d'aquest DNI.

I si ens equivoquem en dos dígits que s'han intercanviat de posició, i escrivim, per exemple, 34**41**9351D? En aquest cas, de nou, en calcular $34419351 = 12$ a $\mathbb{Z}_{23}$, podem detectar l'error ja que 12 correspon a la lletra N.

Finalment, què podem fer si un dels dígits és borrós, per exemple, si tenim 341493□1D on el setè dígit no es reconeix? En aquest cas, podem plantejar l'equació lineal següent a $\mathbb{Z}_{23}$, $14\cdot 3+6\cdot 4+19\cdot 1+18\cdot 4+11\cdot 9+8\cdot 3+10\cdot x_1+1 = 9$, o sigui $10x_1 = 4$ a $\mathbb{Z}_{23}$. Com que l'invers de 10 és 7, tenim que $x_1 = 4\cdot 7 = 28 = 5$ a $\mathbb{Z}_{23}$. Per tant, el dígit de la posició setena és 5 i obtenim el DNI 34149351D.

2.2 Codi ISBN

Cada llibre porta associat un identificador únic, l'anomenat *International Standard Book Number* (ISBN) [27], que consisteix en una seqüència de 10 símbols en què cadascun pot ser un element de $\{0,1,2,3,4,5,6,7,8,9,\mathrm{X}\}$ i X representa el 10. Les operacions es realitzen a $\mathbb{Z}_{11}$, a diferència del codi DNI, que eren a $\mathbb{Z}_{23}$. El darrer símbol representa la redundància i es calcula a partir dels anteriors. Aquest codi també permet detectar si, durant la transcripció d'aquest identificador, s'ha produït un error en algun dels seus dígits o la transposició de dos d'ells [6, 12].

EXEMPLE 3. Els identificadors 0-444-85010-4 i 84-732-9114-X corresponen als codis ISBN dels llibres *The Theory of Error-Correcting Codes*, de Florence J. MacWilliams i Neil J. A. Sloane, en l'editorial North-Holland, i *Mirall trencat*, de Mercè Rodoreda, en l'editorial Club Editor, respectivament.

Dels 10 símbols, els que apareixen abans del primer guió fan referència a l'idioma/país, els símbols entre el primer i el segon guió identifiquen l'editorial, els següents identifiquen el llibre dins de l'editorial, i finalment el darrer representa la redundància. A partir dels nou primers símbols, denotats per x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, es calcula la redundància x_{10} com a $x_{10} = x_1 + 2x_2 + 3x_3 + \cdots + 9x_9$ a $\mathbb{Z}_{11}$. Si el resultat és 10, escrivim el símbol X.

EXEMPLE 4. Continuant amb el primer ISBN que apareix en l'exemple 3, si en escriure'l ens equivoquem en un símbol i escrivim, per exemple, 0-444-85**5**10-4, aleshores en calcular x_{10} obtenim que $x_{10} = 6$ en comptes de 4. Per tant, podem detectar que hi ha hagut un error, i repassar-ne la transcripció. De forma similar, si ens equivoquem en dos símbols consecutius que s'han intercanviat de posició, i escrivim per exemple, 0-444-**58**010-4, de nou en calcular x_{10} obtenim que $x_{10} = 7 \neq 4$ i així detectem que hi ha hagut algun error. Finalment, és fàcil veure que si un dels símbols no es reconeix, podem obtenir-lo resolent una equació lineal a $\mathbb{Z}_{11}$.

2.3 Codi IBAN i CCC

Els comptes bancaris tenen associat un codi, anomenat *International Bank Account Number* (IBAN), que consisteix en una seqüència d'un màxim de 34 ca-

ràcters alfanumèrics que identifiquen, de forma única, un compte bancari d'una determinada entitat financera [24]. Els dos primers caràcters identifiquen el país. Els dos següents són dígits de control que es calculen a partir de la resta, com veurem tot seguit. La resta corresponen al número de compte bancari i permeten identificar també l'entitat i l'oficina, en la majoria de països.

EXEMPLE 5. La seqüència BG18RZBB91550123456789 correspon al codi IBAN d'un possible compte bancari a Bulgària, i la seqüència ES0212345678060111555555 a un a Espanya. A Bulgària tots els codis IBAN tenen exactament 22 caràcters i a Espanya en tenen 24.

Per calcular els dos dígits de control, situats en les posicions tercera i quarta de la seqüència, es procedeix de la forma següent. Les dues primeres lletres corresponents al país es traslladen a les dues darreres posicions, s'eliminen els dos dígits de control i s'afegeixen dos zeros al final. Els caràcters se substitueixen per un número de dues xifres d'acord amb la taula 2 i es calcula el número obtingut a $\mathbb{Z}_{97}$. Finalment, per evitar utilitzar com a dígits de control el 00 i 01, es resta el valor obtingut a 98, i s'obtenen els dos dígits de control. Si el resultat conté un únic dígit, s'afegeix un zero al davant.

10	11	12	13	14	15	16	17	18	19	20	21	22
A	B	C	D	E	F	G	H	I	J	K	L	M
23	24	25	26	27	28	29	30	31	32	33	34	35
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

TAULA 2: Assignació numèrica per a l'IBAN.

EXEMPLE 6. Els dos dígits de control de l'IBAN BG18RZBB91550123456789 són 18. A continuació comprovem que és correcte. Primer, traslladem les dues primeres lletres al final, eliminem els dos dígits de control i afegim dos zeros al final, per tant, obtenim RZBB91550123456789BG00. A continuació, substituint els caràcters per valors numèrics segons la taula 2, arribem al número 27351111915501234567891116 00, que és igual a 80 a $\mathbb{Z}_{97}$. Els dígits de control són efectivament $98 - 80 = 18$.

Com en els dos codis anteriors, el DNI i l'ISBN, el codi IBAN també permet detectar possibles errors produïts en una única posició o transposicions de dos caràcters, així com recuperar-ne un que aparegui il·legible.

A Espanya, el codi IBAN es va implantar definitivament l'1 de febrer del 2014 aprofitant l'antic codi de compte corrent (CCC). De fet, el codi IBAN es construeix a partir del codi CCC, que té 20 xifres decimals, afegint al davant els dos caràcters ES corresponents al país i els dos dígits de control que hem explicat abans, fins a completar els 24 caràcters.

El codi CCC està format per 20 dígits. Els 4 primers dígits identifiquen l'entitat bancària, els 4 següents identifiquen l'oficina, els 2 següents són dígits de control, i finalment els darrers 10 descriuen el número de compte bancari.

Així, aquest codi el podem representar de la manera següent:

$$x_3x_4x_5x_6 \quad x_7x_8x_9x_{10} \quad c_1c_2 \quad y_1y_2y_3y_4y_5y_6y_7y_8y_9y_{10}.$$

El primer dígit de control c_1 es calcula a partir dels 8 dígits anteriors, d'acord amb l'equació següent $c_1 = -\sum_{i=3}^{10} 2^{i-1}x_i = 7x_3 + 3x_4 + 6x_5 + x_6 + 2x_7 + 4x_8 + 8x_9 + 5x_{10}$ a $\mathbb{Z}_{11}$, i el segon c_2, a partir dels 10 dígits següents com a $c_2 = -\sum_{i=1}^{10} 2^{i-1}y_i = 10y_1 + 9y_2 + 7y_3 + 3y_4 + 6y_5 + y_6 + 2y_7 + 4y_8 + 8y_9 + 5y_{10}$ a $\mathbb{Z}_{11}$. Si en fer aquests càlculs obtenim un 10 a $\mathbb{Z}_{11}$, assignem el dígit 1. Fixem-nos que en els dos casos la fórmula és la mateixa considerant que $x_1 = x_2 = 0$ per al càlcul de c_1. Aquests codis tenen les mateixes propietats per detectar errors o corregir un esborrall (dígit borrós que no es reconeix) que els codis anteriors, excepte en alguns casos en què en fer els càlculs obtenim $c_i \in \{1, 10\}$.

EXEMPLE 7. El codi CCC, corresponent al codi IBAN ES0212345678060111555555, és 12345678060111555555, on 1234 representaria una entitat bancària i 5678 una oficina d'aquesta entitat. Si a l'hora de transcriure aquest compte bancari, escrivim 12345678060111**6**55555, aleshores en calcular els dígits de control c_1 i c_2 obtenim que $c_1 = 0$ però $c_2 = 1$ en comptes de 6. Per tant, haurem detectat que hi ha algun error, i que aquest es troba dins dels darrers 10 dígits.

2.4 Codi EAN

La majoria dels productes comercials porten associat un número de 13 xifres decimals anomenat *European Article Number* (EAN) o, més recentment, *International Article Number*. L'EAN apareix just a sota d'un codi de barres que serveix per facilitar-ne la lectura. Els dos o tres primers dígits identifiquen l'estat o associació a la qual està registrat el fabricant, els següents de 5 a 8 dígits identifiquen l'empresa, els següents fins al 12è, el producte, i finalment el darrer és el dígit de control [25, 20].

El dígit de control es calcula a partir dels anteriors. Si l'EAN de 13 xifres el denotem per $x_1x_2\ldots x_{13}$, aleshores x_{13} es calcula de la manera següent: $x_{13} = -\sum_{i=1}^{6}(x_{2i-1} + 3x_{2i}) = 9x_1 + 7x_2 + 9x_3 + 7x_4 + 9x_5 + 7x_6 + 9x_7 + 7x_8 + 9x_9 + 7x_{10} + 9x_{11} + 7x_{12}$ a $\mathbb{Z}_{10}$. Igual que els codis detectors que hem vist en les subseccions anteriors, el codi EAN permet detectar si s'ha produït un error en un dels dígits, però en canvi no permet detectar sempre la transposició de dos dígits. Concretament, si s'intercanvien dos dígits diferents, x_i i x_j, tals que i i j tenen la mateixa paritat, o bé $x_i - x_j = 5$, la transposició no es detecta [6, 20]. També és fàcil veure que podem recuperar un dígit il·legible, ja que l'1 i el 3 (o equivalentment, els seus oposats, el 9 i el 7) són invertibles a $\mathbb{Z}_{10}$.

EXEMPLE 8. Si l'empresa utilitza el codi EAN de l'Associació Espanyola de Codificació Comercial (AECOC), els dos primers dígits són 84. En canvi, en altres països com Alemanya els primers dígits són números del 400 al 440.

coordinates. We compare the concepts used by the MOL with respect to the analytical method of variable separation. We show that the results obtained with the MOL are very good approximations of the analytical solutions.

Keywords: partial differential equations, discretization of a continuous variable, numerical analysis.

MSC2010 Subject Classification: 65M20.

Mercè Villanueva and Cristina Fernández-Córdoba

Error detecting and correcting codes and some of their applications in the information society

In digital transmissions of information from a sender to a receiver through a channel, errors may occur. In this article, the most important concepts and results of the theory of error detecting and correcting codes are discussed. This theory studies efficient methods to guarantee accurate transmission of information. First, some everyday examples of error detecting codes are described, such as the codes included in DNI, ISBN, IBAN and EAN. Next, the classical theory of error correcting codes is presented, particularly considering linear codes and, within them, cyclic codes, which are more efficient for encoding. The two most important families of cyclic codes, the BCH and Reed-Solomon codes, which also make it possible to decode efficiently, are also described. Lastly, two historical applications, in computer memories and the transmission of photographs in space, and two more recent applications, in QR codes and distributed storage, are shown.

Keywords: error detection, error correction, linear codes, cyclic codes, BCH, Reed-Solomon, applications.

MSC2010 Subject Classification: 94B05, 94B15, 11T71.
