

# Sistemas de identificação com algarismos de controlo<sup>1</sup>

Helder Pinto

Os algarismos de controlo servem, essencialmente, para detectar erros quando se lida com números compostos por muitos algarismos. Estes algarismos aparecem nos mais diversos sistemas de identificação como, por exemplo, no Bilhete de Identidade, nos códigos de barras, nas notas de Euro, no Cartão Visa e no NIB (Número de Identificação Bancária).

Estes mecanismos, apesar de passarem a maioria das vezes despercebidos, são extremamente úteis para evitar enganos. Já viu os aborrecimentos que teria se um simples engano na escrita do seu NIB, fizesse com que estivesse a transferir dinheiro para uma pessoa desconhecida? E se um erro semelhante na leitura do Código de Barras, o fizesse pagar uma lata de atum ao preço de uma televisão? São estes algarismos de controlo que permitem que este tipo de erros seja facilmente detectável.

## Bilhete de identidade

O algarismo de controlo que mais tem dado que falar é o existente no Bilhete de Identidade, num pequeno quadrado à direita do respectivo número de identificação (figura 1).

As histórias que circulam à volta deste algarismo têm sido várias, sendo a mais comum dizer-se que este algarismo indica o número de pessoas com o mesmo nome da pessoa titular do respectivo BI. De facto, tal não é verdade. Este algarismo é apenas e só um algarismo de controlo, calculado a partir do número de BI e que permite detectar erros na transcrição destes números. Como é óbvio, este sistema apenas será útil se for aplicado com recurso à tecnologia. A solução ideal seria escrever o número do BI num computador (algarismo de controlo incluído) e este verificar se o número de BI com aquele algarismo de controlo é válido ou não. Se não for, ou houve engano a escrever o número ou o BI em questão é falso.

O algarismo de controlo do BI é calculado a partir do número de identificação resolvendo a equação:

$$9x_1 + 8x_2 + 7x_3 + 6x_4 + 5x_5 + 4x_6 + 3x_7 + 2x_8 + C \equiv 0 \pmod{11}$$

onde  $C$  é o algarismo de controlo,  $x_1$  é o primeiro algarismo mais à esquerda do número de BI,  $x_2$  é o segundo e assim sucessivamente. Aos números de BI que tiverem menos de oito algarismos, deverão ser acrescentados os zeros necessários à esquerda do número, até este perfazer os oito algarismos. Por exemplo, o número 123456 deve ser encarado como 00123456.

Como é fácil verificar, este algarismo de controlo pode tomar 11 valores distintos (0, 1, 2, ..., 10), mas o que seria realmente prático era usar apenas um carácter para identificar cada um deles. E assim, para atingir este objectivo, o que se fez foi substituir o algarismo de controlo dez por zero. Nada mais simples, pois não? Provavelmente não, só que assim perdeu-se a eficácia deste sistema de controlo, uma vez que é impossível distinguir o algarismo de controlo dez do algarismo zero.

Mas existiam muitas outras soluções como, por exemplo, a utilizada pelo ISBN — número de identificação de cada livro e que usa um sistema semelhante ao do BI — onde se substituiu o dez pela letra  $X$  (a lembrar a numeração romana). Assim temos onze caracteres distintos (0, 1, 2, ..., 9,  $X$ ) para os onze possíveis valores do algarismo de controlo.

Outra questão importante quando se concebem sistemas de identificação é a determinação do tipo de erros que estes detectam. Os erros que são cometidos com mais frequência são os denominados erros singulares (engano em apenas um algarismo) e, portanto, para que um sistema de controlo seja realmente útil deverá ter uma eficácia de 100% neste tipo de erros.

Vejamos o exemplo do BI apresentado na figura 1. O algarismo de controlo é zero. E se em vez de 11866607, tivéssemos escrito 11866601? O ideal seria que estes dois nú-

O formulário de identificação (BI) apresentado na figura 1 contém o seguinte conteúdo:

- N.º: 11866607 0 (o zero final está circulado em vermelho)
- EMISSÃO (DELARANCE / ISSUE): [ ]
- NOME (NOM / NAME): [ ]
- PAÍS (PAYS): [ ]
- NATURALIDADE (LIEU DE NAISSANCE / BIRTHPLACE): [ ]
- RESIDÊNCIA (RESIDENCE / RESIDENCE): [ ]
- DATA DE NASCIMENTO (DATE OF BIRTH): [ ]
- ESTADO CIVIL (MARRIAGE STATUS): [ ]
- ALTURA (STATURE / HEIGHT): [ ]
- VALIDADE (VALIDITY / EXPIRATION DATE): [ ]
- INDICAÇÕES EVENTUAIS (INDICATORS / ACCIDENTAL INDICATIONS): [ ]
- MINISTÉRIO DA JUSTIÇA  
DIRECÇÃO-GERAL DOS REGISTOS E DO NOTARIADO  
SERVIÇOS DE IDENTIFICAÇÃO CIVIL

Figura 1. O algarismo de controlo no bilhete de identidade.



Figura 2. Nota de 10 euros.



meros tivessem algarismos de controlo diferentes, mas tal não acontece pois ambos têm como algarismo de controlo o zero. Esta situação surge do facto de se ter substituído o controlo dez pelo zero. De facto, mostra-se que, se tivesse sido escolhido uma letra ou um símbolo para substituir o dez como algarismo de controlo, este erro seria facilmente detectado bem como todos os outros erros singulares. Mostra-se igualmente que, se este sistema tivesse sido correctamente concebido, também todas as transposições consecutivas (troca de dois algarismos consecutivos) seriam detectadas. Como estes dois tipos de erro são os mais frequentes, teríamos um bom sistema de controlo.

### Notas de euro

Um dos mecanismos de segurança das notas de Euro mais desconhecidos é o da formação do número de série, que obedece a certas regras (figura 2).

O número de série que podemos encontrar numa qualquer nota (verdadeira) de Euro é composto por uma letra seguida de onze algarismos. A letra representa o país do qual é proveniente a nota; os dez algarismos seguintes servem para numerar a nota enquanto que o último é um algarismo de controlo semelhante ao do BI.

Letra	País	Valor
L	Finlândia	4
M	Portugal	5
N	Áustria	6
P	Holanda	8
R	Luxemburgo	1
S	Itália	2
T	Irlanda	3
U	França	4
V	Espanha	5
X	Alemanha	7
Y	Grécia	8
Z	Bélgica	9

Vejamus então como determinar este algarismo de controlo. Em primeiro lugar, cada letra que representa um determinado país é conotada com um valor numérico (ver tabela) e,

de seguida, somam-se a esse valor todos os seguintes dez algarismos que compõem o número de série. O algarismo de controlo vai ser o algarismo (1, 2, 3, ... ou 9) que somado ao número anterior, dá origem a um número divisível por nove. Em linguagem matemática, corresponde à solução da seguinte equação:

$$L + x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + x_7 + x_8 + x_9 + x_{10} + C \equiv 0 \pmod{9}$$

onde  $L$  é o valor representado pela letra,  $x_1$  o 1º algarismo,  $x_2$  o 2º algarismo, ... e  $C$  o algarismo de controlo. Que tipos de erro são detectados por este sistema? Em primeiro lugar, nenhuma transposição de dois (ou mais) algarismos é detectada devido à propriedade comutativa da adição (modular) e mesmo os erros singulares não são todos detectados. Se trocarmos um zero por um nove (ou vice-versa) o número de controlo mantém-se inalterado.

### Código de barras

O algarismo de controlo existente no código de barras é o algarismo que se situa mais à direita e é calculado a partir dos restantes doze algarismos do seguinte modo:

$$x_1 + 3x_2 + x_3 + 3x_4 + x_5 + 3x_6 + x_7 + 3x_8 + x_9 + 3x_{10} + x_{11} + 3x_{12} + C \equiv 0 \pmod{10}$$

onde  $C$  é o algarismo de controlo,  $x_1$  é o 1º algarismo mais à esquerda do código de barras,  $x_2$  é o 2º,  $x_3$  é o 3º e assim sucessivamente (figura 3).

Este sistema, apesar de detectar todos os erros singulares, também não é capaz de detectar todas as transposições consecutivas de dois algarismos. Vejamos o caso em que trocamos apenas os dois primeiros algarismos do Código de Bar-

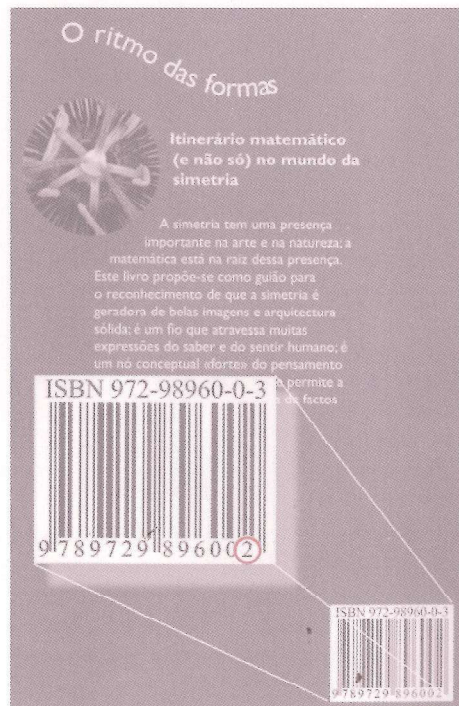


Figura 3.



ras. Na tabela seguinte, podemos ver o valor da soma das parcelas correspondentes a  $x_1$  e a  $x_2$  (em módulo 10), bem como a soma que se obteria se estes dois primeiros algarismos fossem trocados (em baixo):

		$x_2$									
		0	1	2	3	4	5	6	7	8	9
$x_1$	0	00	31	62	93	24	55	86	17	48	79
	1	13	44	75	06	37	68	99	20	51	82
	2	26	57	88	19	40	71	02	33	64	95
	3	39	60	91	22	53	84	15	46	77	08
	4	42	73	04	35	66	97	28	59	80	11
	5	55	86	17	48	79	00	31	62	03	24
	6	68	99	20	51	82	13	44	75	06	37
	7	71	02	33	64	95	26	57	88	19	40
	8	84	15	46	77	08	39	60	91	22	53
	9	97	28	59	80	11	42	73	04	35	66

Como se pode reparar, neste sistema existem várias transposições consecutivas que não são detectadas: a troca de 05 por 50, a troca de 16 por 61, a troca de 27 por 72, a troca de 38 por 83, a troca de 49 por 94 e os seus recíprocos.

### Outros sistemas

A maioria dos sistemas de identificação com algarismos de controlo é baseado na aritmética modular. Apesar de existirem sistemas melhores que os três apresentados (como, por exemplo, o do NIB onde se usam dois algarismos de controlo em vez de um), mostra-se que em qualquer sistema baseado nesta aritmética nunca se vai poder verificar simultaneamente as seguintes condições:

- detectar todos os erros singulares e todas as transposições de algarismos adjacentes;
- usar somente os algarismos 0, 1, 2, ..., 9, sem a necessidade de símbolos extra e que, por uma questão de economia, trabalhem somente com um algarismo de controlo.

Mas o que fazer então para resolver o nosso problema? Em 1969, o matemático holandês J. Verhoeff encontrou um sistema que verifica as condições acima indicadas. A base do sistema criado por Verhoeff é a Teoria dos Grupos (e, em particular, o grupo Diedral  $D_5$ ), que envolve conceitos matemáticos “mais sofisticados” que os utilizados na aritmética modular. Apesar das vantagens evidentes na aplicação do sistema idealizado por Verhoeff, a sua utilização é quase nula. Um dos raros exemplos era o sistema implementado nas notas de marco alemãs, o que torna ainda mais incompreensível o facto de o Euro ter adoptado um sistema de controlo tão fraco (note-se que a sede do Banco Central Europeu é na Alemanha).

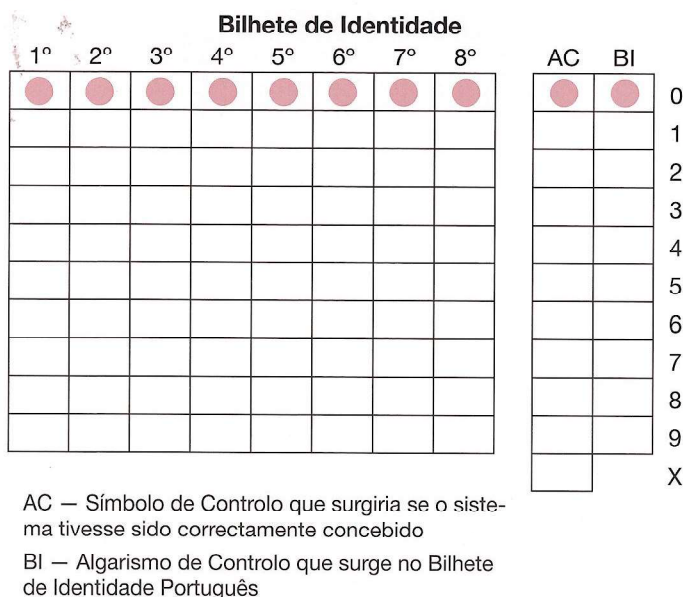


Figura 4.

Na página da internet

[www.atractor.pt/mat/alg\\_controlo/](http://www.atractor.pt/mat/alg_controlo/)

podem-se encontrar mais informações sobre estes e outros sistemas de identificação. Neste mesmo endereço, é possível ainda verificar experimentalmente os tipos de erros que estes sistemas detectam e confirmar se o algarismo de controlo, por exemplo, do seu BI ou das suas notas de Euro estão correctos ou não.

Por exemplo, no BI da figura apresentada anteriormente, verifica-se facilmente que este tem o algarismo de controlo zero devido à simplificação considerada em relação ao controlo dez (figura 4).

Quem não conhece ou não está familiarizado com a aritmética modular, poderá igualmente encontrar, no referido endereço, informação bastante acessível sobre esta temática.

### Notas

- 1 Este trabalho foi realizado sob a orientação do professor Jorge Picado da Universidade de Coimbra, no âmbito de uma Bolsa atribuída pela Fundação Calouste Gulbenkian para desenvolver um projecto de divulgação da Matemática no Atractor.

### Bibliografia

- [1] J. Picado, *A álgebra dos sistemas de identificação*, in Boletim da SPM, n° 44, Abril de 2001, pp.39–73.
- [2] J. Buescu, *O Mistério do Bilhete de Identidade e Outras Histórias*, 9ª ed, gradiva, Lisboa, 2004.
- [3] J. Buescu, *Da Falsificação dos Euros aos Pequenos Mundos*, 2ª ed, gradiva, Lisboa, 2003.
- [4] J. Kirtland, *Identification Numbers and Check Digit Schemes*, The Mathematical Association of America, 2001

Helder Pinto

Associação Atractor. CCVO