Matemática no quotidiano:

Do Cartão VISA ao Número de Identificação Bancária

RICARDO CUNHA TEIXEIRA
Departamento de Matemática da Universidade dos Açores, rteixeira@uac.pt

	0	1	2	3	4	5	6	7	8	9
σ	0	4	3	2	1	6	7	8	9	5
σ^2	0	1	2	3	4	7	8	9	5	6
σ^3	0	4	3	2	1	8	9	5	6	7
σ^4	0	1	2	3	4	9	5	6	7	8
σ^5	0	4	3	2	1	5	6	7	8	9
σ^6	0	1	2	3	4	6	7	8	9	5
σ^7	0	4	3	2	1	7	8	9	5	6
σ^8	0	1	2	3	4	8	9	5	6	7
σ^9	0	4	3	2	1	9	5	6	7	8

*	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	0	6	7	8	9	5
2	2	3	4	0	1	7	8	9	5	6
3	3	4	0	1	2	8	9	5	6	7
4	4	0	1	2	3	9	5	6	7	8
5	5	9	8	7	6	0	4	3	2	1
6	6	5	9	8	7	1	0	4	3	2
7	7	6	5	9	8	2	1	0	4	3
8	8	7	6	5	9	3	2	1	0	4
9	9	8	7	6	5	4	3	2	1	0

$$\sigma^9(2) * \sigma^8(0) * \sigma^7(1) * \sigma^6(0) * \sigma^5(3) * \sigma^4(4) * \sigma^3(5) * \sigma^2(7) * \sigma(1) * ?$$

$$= 3 * 0 * 4 * 0 * 2 * 4 * 8 * 9 * 4 * ? = 1 * ? = 0$$

A implementação de números de identificação com algarismo de controlo (*check digit*) permite detetar erros que possam ocorrer na escrita, transmissão ou leitura da informação, sempre que lidamos com sequências de vários algarismos.

Os erros mais comuns são os singulares (quando escrevemos o algarismo "a" em vez do algarismo "b"), as transposições de algarismos adjacentes (quando escrevemos "ab" em vez de "ba", por exemplo, ao premir as teclas do computador pela ordem errada), as transposições intercaladas ("acb" em vez de "bca"), os erros gémeos ("aa" em vez de "bb") e os erros gémeos intercalados ("aca" em vez de "bcb"). A frequência com que estes erros ocorrem é diferente. No livro "Error detecting decimal codes", Verhoeff apresenta frequências relativas para as diferentes situações: erros singulares (79,1%),transposições de algarismos adjacentes (10,2%),transposições intercaladas (0,8%), erros gémeos (0,5%) e erros gémeos intercalados (0,3%). O autor atribui ainda uma percentagem de 0,5% para erros fonéticos e de 8,6% para erros aleatórios. Deste estudo sobressai um facto interessante: cerca de 90% dos erros que ocorrem na escrita de uma sequência de algarismos são erros singulares ou transposições de algarismos adjacentes.

Existem diferentes tipos de sistemas de identificação com *check digit*. A escolha do algoritmo a implementar deve satisfazer dois princípios: por um lado, é importante escolher um sistema eficaz que detete o maior número possível de erros; por outro lado, a sua utilização no terreno deve ser de alguma forma acessível, particularmente para quem tem de lidar diariamente com os números produzidos por esse algoritmo. Hoje em dia a utilização de meios eletrónicos revela-se muito eficaz, quer para gerar o algarismo de controlo de novos números, como para validar números que já se encontrem em circulação. Mesmo assim, há uma série de requisitos importantes a ter em conta quando se pretende implementar um novo sistema de identificação. Desde logo, a escolha do alfabeto, ou seja, dos símbolos a utilizar. Normalmente, opta-se por recorrer apenas aos dez algarismos vulgarmente utilizados, do 0 ao 9. É o caso do exemplo que se segue.

O método desenvolvido pela IBM, também conhecido por algoritmo de Luhn, aplica-se à generalidade dos cartões de crédito: VISA e VISA Electron (em que o primeiro algarismo da esquerda é um 4), MarterCard (5), AmericanExpress (3) e Discover (6), entre outros.

Considere-se o número de um cartão VISA: 4188360045386426. Como é habitual, o algarismo de controlo é o primeiro algarismo da direita, ou seja, o algarismo das unidades (6). Para verificar se este número é válido, procede-se da seguinte forma: fazendo a leitura do número da direita para a esquerda (isto porque se deve começar pelo algarismo de controlo), adicionam-se todos os algarismos que estão nas posições ímpares (primeiro algarismo, terceiro algarismo,…). Obtemos s1=6+4+8+5+0+6+8+1=38. Em seguida, multiplicamos por 2 os algarismos nas posições pares (segundo algarismo, quarto algarismo,…). Ficamos com 2x2=4; 2x6=12; 2x3=6; 2x4=8; 2x0=0; 2x3=6; 2x8=16; 2x4=8. Na etapa seguinte, adicionamos os algarismos dos números obtidos (note-se que não se adicionam os números obtidos, mas sim os seus algarismos). Obtemos s2=4+1+2+6+8+0+6+1+6+8=42. Por fim, calcula-se o valor da soma de teste s=s1+s2=38+42=80, que deverá ser um múltiplo de 10 (ou seja, o seu algarismo das unidades deverá ser 0). Se o resultado final não for um múltiplo de 10, significa que ocorreu um erro e que o número não está correto. Um método alternativo para adicionar os algarismos consiste em retirar "dezes" sempre que possível. O resultado final terá que ser 0 (significa que a soma de teste é um múltiplo de 10, ou seja, que o resto da sua divisão por 10 é zero).

A atribuição de um algarismo de controlo aos números que identificam os cartões de crédito reveste-se de particular importância, pois permite detetar erros que, de outra forma, promoveriam o caos nas contas de muita gente. Mas será que o algoritmo de Luhn deteta todos os erros mais comuns? O sistema deteta 100% dos erros singulares e 97,8% das transposições de algarismos adjacentes. Apenas não é detetada a trocados algarismos 0 e 9. Por exemplo, o número4188360076096597 e o que se obtém pela troca dos algarismos 0 e 9, 418836007690 6597, apresentam a mesma soma de teste (80), que é um múltiplo de 10, pelo que o erro não é detetado. Este sistema também não deteta transposições intercaladas.

Há um algoritmo mais eficaz desenvolvido por Verhoeff, em 1969, que utiliza os mesmos símbolos (os algarismos do 0 a 9).Este sistema deteta100% dos erros singulares, 100% das transposições de algarismos adjacentes e algumas das transposições intercaladas. Paradoxalmente, é um método pouco utilizado, talvez por necessitar de uma maior bagagem matemática. O algoritmo de Verhoeff recorre ao grupo diedral D5 das simetrias de um pentágono regular, o mesmo grupo de simetria das estrelas em calçada, localizadas no Largo da Matriz, em Ponta Delgada (o grupo apresenta 5 simetrias de rotação e 5 simetrias de reflexão). Estamos perante uma interessante ponte de ligação com o conceito de simetria, o que é um exemplo do poder de abstração e de sistematização da Matemática, que se traduz na capacidade de encontrar propriedades comuns em coisas que, à primeira vista, não têm qualquer ligação.

Durante vários anos, o Deutsche Bundesbank recorreu ao trabalho desenvolvido por Verhoeff para identificar as notas alemãs, antes da entrada no Euro. Atualmente, a Universidade de Coimbra utiliza um algoritmo similar para gerar, por exemplo, os números de aluno e os códigos das disciplinas. Este facto deve-se ao trabalho desenvolvido por Jorge Picado, professor da Universidade de Coimbra. Os interessados poderão consultar o seu artigo, "A álgebra dos sistemas de identificação: da aritmética modular aos grupos diedrais", publicado no Boletim da Sociedade Portuguesa de Matemática em 2001.

Na imagem, ilustra-se um exemplo de aplicação deste algoritmo para determinar o algarismo de controlo do número 201034571? (o ponto de interrogação representa o algarismo de controlo, por enquanto, desconhecido). Em primeiro lugar, aplica-se uma permutação a cada algarismo, de acordo com a fórmula apresentada na imagem e a tabela da esquerda (a tabela apresenta os valores resultantes de compor sucessivamente a permutação definida na primeira linha). A leitura da tabela processa-se da mesma forma como se tivéssemos a jogar ao tradicional jogo da batalha naval. Assinalámos as entradas da tabela utilizadas na aplicação da fórmula.

Depois de permutar os algarismos, obtemos uma expressão constituída por novos algarismos, do 0 ao 9, separados pelo símbolo *, que representa a operação binária do grupo D5, ou seja, uma função que a cada par de algarismos faz corresponder um novo algarismo de acordo com a tabela da direita, que pode ser lida novamente como se de um jogo da batalha naval se tratasse. Façamos os cálculos da esquerda para a direita, seguindo o sentido normal de leitura. Tem-se 3*0=3 (a linha do 3 e a coluna do 0 intersectam-se no 3). Da mesma forma, 3*4=2 (a linha do 3 e a coluna do 4 intersectam-se no 2). Segue-se 2*0=2, 2*2=4, 4*4=3, 3*8=6, 6*9=2 e 2*4=1. Ficamos com 1*?=0. Ao observar com atenção a linha do 1, apercebemo-nos que o 0 pertence à coluna do 4, pelo que terá que ser 1*4=0. Sendo assim, 4 é o algarismo de controlo que pretendíamos determinar!

Se nos predispusermos a alargar o alfabeto de símbolos ou a considerar mais de um algarismo de controlo, podemos obter algoritmos ainda mais eficazes na deteção de erros. É o caso dos algoritmos estabelecidos pela norma ISO/IEC 7064. Por exemplo, o algoritmo MOD 11-2 é utilizado para identificar as receitas médicas em Portugal e utiliza um símbolo adicional (o X, que representa o número 10). Já o algoritmo MOD 97-10 requer a utilização de dois algarismos de controlo e é empregue na emissão do Número de Identificação Bancária (NIB). O NIB é composto por 21 algarismos, da esquerda para a direita: os 4 primeiros identificam o banco a que pertence a conta; os 4 seguintes, o balcão ou agência; os 11 que se seguem, o número de conta propriamente dito; e os 2 últimos são algarismos de controlo, escolhidos de forma a que a divisão do NIB por 97 dê resto 1. Este sistema é bastante eficaz. Deteta 100% dos erros singulares, 100% das transposições de algarismos adjacentes e 100% das transposições intercaladas.

Da próxima vez que fizer uma transferência bancária, não fique preocupado em confirmar repetidas vezes que não se enganou na escrita do NIB, pois se cometer um erro a probabilidade de ele ser detetado é bastante elevada. E tudo isso graças à Matemática!