Error Detecting Codes

An online book shop sells books. Each book has a four digit code-number. To order a book you have to type this code-number into an online order form. But you might make an error when you do this.

Say the book you want to buy has code-number 4693.

You might type in 4673 instead of 4693. This is a digit error.

You might type in 4963 instead of 4693. This is a swap error.

If you make an error then you get sent the wrong book. It would be great if the shop could detect these errors. There are many ways to do this. We will look at the check-digit method.

Example 1

Sum of digits method:

We add a check-digit at the end of each four digit code-number. So now each book has a five digit code-number. The check-digit is chosen so that the sum of the digits is a multiple of 10.

If a book has code-number 3725, then the check-digit is 3 because $3+7+2+5+3=20=2\times10$

This book now has code-number 37253

If you make a digit error and type in 37283, then this will be detected because the sum of the digits is no longer a multiple of 10 note: $3+7+2+8+3=23$

The shop will not send you the wrong book because 37283 does not correspond to any book. The shop will know you have made an error and will ask you to re-order.

If you make a swap error and type in 32753, then this will not be detected because the sum of the digits is still a multiple of 10 note: $3+2+7+5+3=20$

The shop will send you the wrong book.

Example 2

Weighted sum of digits method:

We add a check-digit at the end of each four digit code-number. So now each book has a five digit code-number. The check-digit is chosen so that the weighted-sum of the digits is a multiple of 10.

If a book has code-number 3725 and if we use the weights: 1, 3, 1, 3, 1

	3	7	2	5	?
weight	1	3	1	3	1

then the check-digit is 9 because $(3\times1)+(7\times3)+(2\times1)+(5\times3)+(9\times1)=50=5\times10$

The book now has code-number 37259

If you make a digit error and type in 37659

	3	7	6	5	9
weight	1	3	1	3	1

then this will be detected because $(3\times1)+(7\times3)+(6\times1)+(5\times3)+(9\times1)=54$

If you make a swap error and type in 37529

	3	7	5	2	9
weight	1	3	1	3	1

then this will be detected because $(3x1)+(7x3)+(5x1)+(2x3)+(9x1)=44$

Example 3

If a book has code-number 3521 and we are using the weights: 1, 4, 1, 4, 1

then the check-digit is 1.

The book now has code-number 35211.

If you make a digit error and type in 35261

	3	5	2	6	1
weight	1	4	1	4	1

then this will not be detected.

In the code-number, you replaced 1 by 6. The digit has changed by 5.

In the weighted sum, you replaced (1×4) by (6×4) The difference is $5\times4=20$

The weighted sum has changed by a multiple of 10 and so the error will not be detected.

So for digit errors:

If the digit changes by 5 and the weight is a multiple of 2

Or

If the digit changes by a multiple of 2 and the weight is 5

then the error will not be detected.

So we avoid using 2, 4, 5, 6, 8 as weights, and use 1, 3, 7, 9 instead. This means all digit errors will be detected.

We also use different weights on adjacent digits so that most swap errors are detected.

Example 4

If a book has code-number 4273 and we are using the weights: 1, 9, 1, 9, 1

then the check-digit is 4.

The book now has code-number 42734

If you make a swap error and type in 47234

	4	7	2	3	4
weight	1	9	1	9	1

then this will not be detected.

In the code-number you swapped 2 and 7. The difference between these digits is 5.

In the weighted sum, you replaced $(2\times9)+(7\times1)$ by $(7\times9)+(2\times1)$ The difference is 40.

The weighted sum has changed by a multiple of 10 and so the error will not be detected.

So for swap errors:

If the digits that are swapped differ by 5 and their weights differ by a multiple of 2 (which they will if we only use 1, 3, 7, 9 as weights) then the error will not be detected.

There are lots of other check-digit methods. For example, some books have a 10 digit ISBN number. The book, Symmetry by Hermann Weyl has the number 0691023743

The last digit is the check-digit. This is calculated as follows:

ISBN	0	6	9	1	0	2	3	7	4	3
weight	10	9	8	7	6	5	4	3	2	1

The weighted sum is:

$(0\times10)+(6\times9)+(9\times8)+(1\times7)+(0\times6)+(2\times5)+(3\times4)+(7\times3)+(4\times2)+(3\times1)=187$

The check-digit is chosen so that this weighted sum is divisible by 11.

If the check-digit is 10 then it is denoted by X in the ISBN code.

Error Correcting Codes

Your space probe is approaching Pluto. It takes a black and white photo and sends it back to Earth. The photo is made up of pixels. Each pixel can be one of sixteen grey-levels. Each grey-level is represented by a 4-digit binary-string. So 0000 represents a white pixel, 1111 represents a black pixel and all the other binary-strings represent shades of grey in-between.

Here are the sixteen possible binary-strings:

0000, 0001, 0010, 0011, 0100, 0101, 0110, 0111, 1000,1001, 1010, 1011, 1100, 1101, 1110, 1111

Back on Earth, you receive a sequence of binary-strings, each binary-string telling you the grey-level of a pixel.

There might be transmission errors. The space probe sends a 0 and you receive a 1 or the space probe sends a 1 and you receive a 0. We want to detect these errors. But if we detect an error, we can't tell the space probe to go back and take the photo again. We need a way to correct the error.

We are going to add 3 extra digits at the end of each binary-string. Richard Hamming came up with a clever way to do this. Here are the sixteen binary-strings with their extra digits added on:

0	0	0	0	0	0	0
0	0	0	1	0	1	1
0	0	1	0	1	1	0
0	0	1	1	1	0	1
0	1	0	0	1	0	1
0	1	0	1	1	1	0
0	1	1	0	0	1	1
0	1	1	1	0	0	0
1	0	0	0	1	1	1
1	0	0	1	1	0	0
1	0	1	0	0	0	1
1	0	1	1	0	1	0
1	1	0	0	0	1	0
1	1	0	1	0	0	1
1	1	1	0	1	0	0
1	1	1	1	1	1	1

We call these our good-strings.

Take any two good-strings, for example, 0010110 and 1011010
To change the first good-string into the second good-string you have to change three of the digits. The first one, the fourth one and the fifth one.
Hamming chose the extra digits so that to change any good-string into any other good-string you have to change at least three of the digits.

1001100 is a good-string.
If you change just the first digit you get 0001100
If you change just the second digit you get 1101100
…
If you change just the seventh digit you get 1001101
We call these strings the bad-neighbours of 1001100
1001100 has seven bad-neighbours.

1011010 is another good-string.
1011010 has seven bad-neighbours.

good-string	good-string
1001100	1011010
bad-neighbours	bad-neighbours
0001100	0011010
1101100	1111010
1011100	1001010
1000100	1010010
1001000	1011110
1001110	1011000
1001101	1011011

Can a bad-neighbour of 1001100 also be a bad-neighbour of 1011010?
If yes, then we could start with 1001100, change one digit to get a bad-neighbour and then change one more digit to get 1011010. We would have changed a good-string into another good-string by changing just two digits. We know this is not possible.
So a bad-neighbour of one good-string cannot be a bad-neighbour of another good-string.
We have sixteen good-strings and each good-string has seven bad-neighbours making a total of 128 different strings. This accounts for every possible 7-digit binary-string.

So every binary-string is either a good-string or a bad-neighbour.
So every binary-string is either a good-string or one digit change away from a good-string.

Back on Earth you receive the string 1010011
This is not a good-string. An error has occurred. We assume that only one digit has been corrupted.
If errors are very rare then this seems reasonable.
We correct this error by replacing 1010011 by the good-string 1010001 which is only one digit change away.

Error correcting codes are useful whenever we want to store or transmit digital data.