

MATHEMATICS FOR MOBILE PHONES AND EFTPOS

Kaye Stacey

University of Melbourne

This article describes some of the mathematics behind the digital revolution. It is common knowledge that the digital revolution involves storing and transmitting messages, information or data as numbers instead of more directly as physical quantities. Why is it, though, that this results in better technology? Why, for example, is compact disc sound better than the sound of a record or a tape recorder? Clearly, the answers to questions like this depend on much more than mathematics, but mathematics plays an important role. This article discusses one of the ways in which mathematics is involved. Two key concepts will be explained—error detecting codes and error correcting codes—and illustrated with two familiar examples—barcodes and ISBN numbers. Finally, a brief introduction to more sophisticated codes will be given.

Finding and correcting errors

A modern way of looking at a variety of devices is as creators, transmitters, stores and receivers of information. A telephone, for example, takes spoken words as information and transmits this information through other intermediate devices to another telephone which receives the information and turns it back into real sound. A telephone measures the human voice about 8000 times a second. Each of these samples is turned into a 'number' between 0 and 255. These numbers are represented in reality by electric current in an on-off binary digit system, but this is not important for the central ideas of this article. These 'numbers' are then transmitted through many other devices in the telephone system.

Along the way, there are many possibilities for these numbers to be changed. There may be electrical interference from other signals as a message travels along a wire. If it travels up to a satellite, there may be lightning. There may be dirt and poor connections in places. If it is stored, it may be affected by radiation. There are many opportunities for the signal to be corrupted. The telephone system is not special in this way. All information transmission and storage systems are subject to errors, although the type of errors that are most likely will vary from situation to situation. A tape recorder may have a dirty head and read information incorrectly. The magnetic information on the tape may have been affected by other magnetic fields. A credit card being swiped through a machine may be bent or scratched.

The advantage of digital information is that errors can be detected and they can very often be fixed. To do this, the mathematical theory of codes is used. Error detecting codes find whether there are errors. Error correcting codes can fix some of them. Making good codes is an important modern application of mathematics, using both old and new ideas. The clarity of modern telephone calls and the lack of hiss in compact disc music are due to the most common errors in the system being detected and then corrected. This is because computation can be carried out on the numbers that make up digital information.

Barcodes on supermarket items – an error detecting code

Codes are used when transmitting digital information to make sure that the information is as accurate as possible. The barcode is a common example of an error detecting code. Supermarkets want barcodes so that the shop computer can quickly identify the item, display the price and record that the item has been sold so that more can be ordered. It is not a particularly powerful code but it is suitable for the situation where it is used.

Barcodes are thick and thin black and white stripes. Modern barcodes represent 13 numbers, from 0 to 9. When the sales assistant scans the item, the 13 numbers are read. But sometimes the computer knows that there is an error and then it beeps and the sales assistant has to scan it again. There are many reasons why there might be an error reading a barcode. Perhaps one of the stripes was not properly drawn from the beginning. The package might be crumpled or folded. Perhaps the

condensation on frozen goods makes it hard to read. But how does the scanner know that there has been an error?

Supermarket barcodes actually have 12 digits containing the information required (country, manufacturer, type of goods etc) and the last one is a 'check digit'. The check digit is calculated from the other ones in this way:

Add up the first plus 3 times the second plus the third plus three times the fourth plus the fifth and so on until three times the twelfth. Then choose the thirteenth digit so that it makes all of this add up to a number ending in zero.

We will use the barcode 9 300650 654013 for Vegemite as an example. Add the first, third, fifth etc: $9 + 0 + 6 + 0 + 5 + 0 = 20$. Then the alternate digits are added and the total is multiplied by 3: $3 + 0 + 5 + 6 + 4 + 1 = 19$ and $19 \times 3 = 57$. Since $20 + 57 = 77$, the check digit needs to be 3 (as it is) to make a sum of 80, a multiple of ten. In the language of congruence, the sum must be congruent to 0 (modulo ten). A barcode reader that reads the thirteen digits can carry out the computation to test for an error. If there is an error in any one of the digits, the sum will not be a multiple of ten and the test will detect the error. Had the barcode been entered by hand, a transposition of two adjacent digits would have been a likely error. Most transpositions (but not all) would have been detected by this test. However, when an error is identified we do not know what it is. If the sum had been 81 instead of 80, any of the digits in the first total could have been out by one, any of the digits in the second sum could have been out by 7 (readers can check why this is) or the check digit itself may have been read incorrectly. Alternatively, there could have been more than one error. This is a simple error detecting code, which suits its purpose well. It identifies many errors. It cannot correct errors, but it is used in a situation where correction is not important—it is simple enough to request the information again.

A supermarket barcode is based on the mathematical theory of congruence modulo ten. This is old mathematics that has found new applications. To show how the theory of congruence is used, it is useful to see which transpositions (2 adjacent digits interchanged) can be detected.

If the first two numbers were interchanged, giving 3 900650 654013, the test sum would be

$20 + 57 + 3$	$-(9 + 3 \times 3)$	$+ 3 + 9 \times 3$
correct sum	minus previous contribution from first two digits	add new contribution from transposed digits

This new sum is equal to 92, which is not a multiple of ten. This error would therefore be detected.

However, if the sixth and seventh numbers were interchanged, giving 9 300605 654013, the test sum would be

$20 + 57 + 3$	$-(0 + 5 \times 3)$	$+ 5 + 0 \times 3$
correct sum	minus previous contribution from those two digits	add new contribution from transposed digits

This new sum is equal to 70, which is a multiple of ten. This error would therefore not be detected.

Generally, if two adjacent digits p and q are interchanged, the test sum would be

$20 + 57 + 3$	$-(p + q \times 3)$	$+ q + p \times 3$
correct sum	minus previous contribution from those two digits	add new contribution from transposed digits

This new sum is equal to $80 - (p + q \times 3) + q + p \times 3 = 80 + 2p - 2q = 80 + 2(p - q)$.

This is a multiple of ten, if $2(p - q)$ is a multiple of ten.

Because $10 = 2 \times 5$, $2(p - q)$ is a multiple of ten if $(p - q)$ is a multiple of 5. Because p and q are digits from 0 to 9, this is only the case if their difference actually is 0 or 5. If the difference is 0, the two numbers are the same and so the transposition is of no account. This means that a transposition error is not detected if and only if the digits differ by 5. If they do not differ by 5, then the error is detected. This is one example of how the factors of ten play an important role in the properties of this code. Barnett (1995) provides an excellent reference to this material.

ISBN numbers – another type of check digit

The system of ISBN numbers is used to identify books all around the world. It is another example of a code that can always detect one error. For example, Barnett's book (1995) which contains a highly readable chapter on codes from which a lot of this information was derived, has the ISBN number 0-13-834094-3. The first digits indicate the country, language and publisher and the later ones the actual book. The last digit is a check digit, which is one of the numbers 0 to 9 or X, which stands for 10. Let the digits of the ISBN number be $x_1, x_2, x_3, x_4, \dots$ up to x_{10} which is the check digit.

The check digit is chosen so that $1x_1 + 2x_2 + 3x_3 + 4x_4 + 5x_5 + \dots + 10x_{10}$ is a multiple of 11. The extra symbol X is needed because sometimes it will be necessary to add ten to get a multiple of eleven.

For example, if the ISBN number is 0-13—834094-3 the test sum is $1 \times 0 + 2 \times 1 + 3 \times 3 + 4 \times 8 + 5 \times 3 + 6 \times 4 + 7 \times 0 + 8 \times 9 + 9 \times 4 + 10 \times 3 = 220$, which is a multiple of 11. This ISBN number passes the test and so it is unlikely that there has been an error.

This example has been included to show another of the many ways of designing check digits. However this bar code is more powerful than the supermarket code. Like the barcode it can detect any single error, but it can also detect any transposition.

For example, if the n th and $(n+1)$ th numbers p and q were interchanged, the test sum would be

correct sum	$-(np + (n+1) \times q)$	$+ n \times q + (n+1) \times p$
correct sum	minus previous contribution	add new contribution
	from those two digits	from transposed digits

This new sum is equal to

correct sum $-(np + (n+1) \times q) + n \times q + (n+1) \times p = \text{correct sum} + p - q = \text{multiple of } 11 + (p-q)$.

However, the difference between two numbers from 0 to X cannot be a multiple of 11. This means that the transposition is always detected. This is an important property, because typing numbers often produces transposition errors.

The ISBN code can detect transpositions because each position has a different multiplier (1 for the first, 2 for the second etc). Because 11 is a prime number, this can be done whilst at the same time preserving the possibility of detecting single errors. If the n th number is read incorrectly as q instead of p then the test sum is

correct sum	$-(np)$	$+ n \times q$
correct sum	minus previous contribution	add new contribution

The new sum is equal to correct sum $- np + nq = \text{multiple of } 11 + n(p-q)$.

For this to be a multiple of 11, $n(p-q)$ must be a multiple of 11. Because 11 is a prime number, this means that either n is a multiple of 11 or $(p-q)$ is a multiple of 11. But both are numbers between 0 and 10. Hence n may be 0 (actually impossible) or $p = q$, which means that there has been no mistake. This depends on the fact that 11 is a prime number. The barcode system could not be used in this way, because it is based on 10, and its factors could combine to make undetected single errors.

Codes that find errors and fix them

The barcode is a simple code that performs well enough in the situation where it is used. As long as a large percentage of the common errors are detected, the code is doing its job. Requesting the information again is a simple way of fixing errors made when scanned items, dragging credit cards through card readers etc. There are, however, other situations, where asking for the information again is not desirable. Information may, for example, have to use a very busy link where it is important to minimise the traffic or it may have to travel a long way, even from another planet. The information may not even still exist. For these situations, codes have been developed which not only detect a large percentage of the errors, but can also fix many of them. These are called error-correcting codes. There are many different types and they are used in many situations, including the memory banks of computers, in medium and long distance telephones, in data links between banks,

and in CDs so that the music sounds excellent as you play it. Stacey (1998) explains a simple error-correcting extension of the ISBN code.

Making good error correcting codes relies on two things: very advanced mathematics and knowing what the errors are probably going to be like. Errors often, for example, occur in bursts. Lightening can cause bursts of errors in signals being transmitted by satellite. If there is an error in one place, then it is likely that the places near it will have errors. Error bursts are also likely when the laser light in a CD player reads the information from a CD. The information is stored in groups (eg. 7 groups of 3) and if one digit in a group of 3 is wrong, it is likely that the other two are as well. A CD player reads about 1.5 million digits per second of audio information. These directly encode the music of the CD. However about twice as many bits of information are used in various aspects of control, including the error-correcting capacity, which results in the exceptionally high quality sound. The coding procedures to recover from the type of errors likely to be encountered in CD's were discovered only a few years before CD's were produced commercially. Barnett (1995) gives details.

More sophisticated codes

The most sophisticated codes are based on mathematics that is quite new and much remains to be discovered about them. In fact, there are many different families of codes, made for different purposes. They are based on mathematical insights from the areas of number theory (as above), geometry, algebra of polynomials, matrices, statistics and other fields. Other codes are harder to explain in a short article, but the references given are useful.

Some codes are built by thinking about geometry in higher dimensional spaces. For example, modems that use Trellis Coded modulation are using a code that is built from the best way that 8 dimensional spheres can be packed in rows in 8 dimensional space. The code words are made to represent the centres of spheres in 8 dimensional space. Problems of packing higher-dimensional spheres are of interest now for many sorts of telecommunications. For example, Conway and Sloane (1988) explain how engineers working on mobile radio needed to know how many 100 dimensional spheres of radius 0.43 can be fitted into a sphere of radius 1 in 100 dimensional space. The mathematical theory of many dimensions seems on the surface an abstract and unreal theory, but is now commercially valuable.

Barnett (1995) describes an important application of codes developed from geometry in higher dimensional space to dramatically improve the reliability of computer memories. The plastic packaging of memory chips contains very small numbers of radioactive molecules. The radiation that can be released from one of these radioactive molecules is enough to alter the contents of a memory cell. Any one memory cell in a memory bank is incredibly reliable. The expected time they could individually operate as memory cells is over a million years. But because a memory bank consists of so many of them (about 8 million in 8 MB), the chance of a failure somewhere is quite large. In fact, the expected time that the memory bank as a whole would last is only 43 days—far too short for practical purposes. The solution to this problem is provided by incorporating a code (with 7 check digits) into the memory bank. As there is more memory, this would increase the chance of memory cells being hit by radiation to about 36 days. However, because the code can fix most common errors the frequency of errors in the memory bank comes down to about one every 63 years—a very practical improvement.

There are many different types of codes and many different branches of mathematics are used to develop codes that are good in different circumstances. Here only the simplest have been described. As our students talk casually of encryption for their home computers, it is good that they know that this is mathematics being used in the real world.

References

- Barnett, S. (1995). *Some modern applications of mathematics*. Hemel Hempstead: Ellis Horwood.
Conway, J. H. & Sloane, N. J. A (1988.) *Sphere packings, lattices and groups*. New York: Springer-Verlag.

Stacey, K. (1998). Error detecting and error correcting codes: the new mathematics of shopping.
Australian Mathematics Teacher. 54(2), 24 – 28.