A oCmedy of Errosr

Dr. Dan Fretwell
Heilbronn Institute for Mathematical Research
University of Bristol
(daniel.fretwell@bristol.ac.uk)

Being a mathematician in normal society...

- I was rubbish at maths in school...
- Oh so you just sit around adding numbers all day?
- Hasn't maths been done already?!
- Isn't maths useless in real life?

Being a mathematician in normal society...

- I was rubbish at maths in school...
- Oh so you just sit around adding numbers all day?
- Hasn't maths been done already?!
- Isn't maths useless in real life?

Being a mathematician in normal society...

- I was rubbish at maths in school...
- Oh so you just sit around adding numbers all day?
- Hasn't maths been done already?!
- Isn't maths useless in real life?

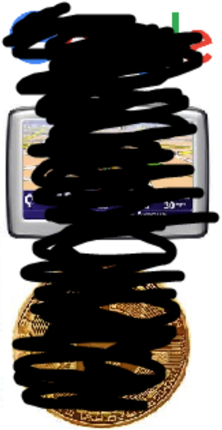
Being a mathematician in normal society...

- I was rubbish at maths in school...
- Oh so you just sit around adding numbers all day?
- Hasn't maths been done already?!
- Isn't maths useless in real life?

Then how do these important things work?

Today: Roughly how these work:

0 36000 29145 2



The English language is bad for transmitting info accurately!

Fair enough, some errors can be corrected:

"Fancy a cheeky pint at the Hen and hCicken on Monday?
Of course you do...see you at 3am."

hCicken $\longrightarrow$ Chicken

The English language is bad for transmitting info accurately!

Fair enough, some errors can be corrected:

"Fancy a cheeky pint at the Hen and hCicken on Monday?
Of course you do...see you at 3am."

hCicken $\longrightarrow$ Chicken

However, some can only be detected:

"Fancy a cheeky pint at the Hen and hCicken on Monday? Of course you do...see you at 3am."

You know that 3am must be wrong but there are at least two possibilities:

3am $\longrightarrow$ 3pm OR 10am

Some can't even be detected:

"Fancy a cheeky pint at the Hen and hCicken on Monday?
Of course you do...see you at 3am."

Monday is a valid day but the Hen and Chicken opens on other days too!

Outline of talk

1. A magic trick
2. Error Correcting Codes
3. Back to the trick

Choose an integer in the range 0-15.

Would you be impressed if I could guess it in 16 Yes/No questions?

Thought not! Instead i'll guess it in 4.

Choose an integer in the range 0-15.

Would you be impressed if I could guess it in 16 Yes/No questions?

Thought not! Instead i'll guess it in 4.

Choose an integer in the range 0-15.

Would you be impressed if I could guess it in 16 Yes/No questions?

Thought not! Instead i'll guess it in 4.

1. Is your number in the set $\{8, 9, 10, 11, 12, 13, 14, 15\}$?
2. Is your number in the set $\{4, 5, 6, 7, 12, 13, 14, 15\}$?
3. Is your number in the set $\{2, 3, 6, 7, 10, 11, 14, 15\}$?
4. Is your number in the set $\{1, 3, 5, 7, 9, 11, 13, 15\}$?

1. Is your number in the set $\{8, 9, 10, 11, 12, 13, 14, 15\}$?
2. Is your number in the set $\{4, 5, 6, 7, 12, 13, 14, 15\}$?
3. Is your number in the set $\{2, 3, 6, 7, 10, 11, 14, 15\}$?
4. Is your number in the set $\{1, 3, 5, 7, 9, 11, 13, 15\}$?

1. Is your number in the set $\{8, 9, 10, 11, 12, 13, 14, 15\}$?
2. Is your number in the set $\{4, 5, 6, 7, 12, 13, 14, 15\}$?
3. Is your number in the set $\{2, 3, 6, 7, 10, 11, 14, 15\}$?
4. Is your number in the set $\{1, 3, 5, 7, 9, 11, 13, 15\}$?

1. Is your number in the set $\{8, 9, 10, 11, 12, 13, 14, 15\}$?
2. Is your number in the set $\{4, 5, 6, 7, 12, 13, 14, 15\}$?
3. Is your number in the set $\{2, 3, 6, 7, 10, 11, 14, 15\}$?
4. Is your number in the set $\{1, 3, 5, 7, 9, 11, 13, 15\}$?

How does this work?

Encode the number as a “word” of length 4 (binary):

$0 \to 0000$	$8 \to 1000$
$1 \to 0001$	$9 \to 1001$
$2 \to 0010$	$10 \to 1010$
$3 \to 0011$	$11 \to 1011$
$4 \to 0100$	$12 \to 1100$
$5 \to 0101$	$13 \to 1101$
$6 \to 0110$	$14 \to 1110$
$7 \to 0111$	$15 \to 1111$

How does this work?

Encode the number as a “word” of length 4 (binary):

$0 \to 0000$	$8 \to 1000$
$1 \to 0001$	$9 \to 1001$
$2 \to 0010$	$10 \to 1010$
$3 \to 0011$	$11 \to 1011$
$4 \to 0100$	$12 \to 1100$
$5 \to 0101$	$13 \to 1101$
$6 \to 0110$	$14 \to 1110$
$7 \to 0111$	$15 \to 1111$

The four questions told me the digits in the “word”.

E.g Is your number in the set $\{8, 9, 10, 11, 12, 13, 14, 15\}$?

$0 \to 0000$	$8 \to 1000$
$1 \to 0001$	$9 \to 1001$
$2 \to 0010$	$10 \to 1010$
$3 \to 0011$	$11 \to 1011$
$4 \to 0100$	$12 \to 1100$
$5 \to 0101$	$13 \to 1101$
$6 \to 0110$	$14 \to 1110$
$7 \to 0111$	$15 \to 1111$

The four questions told me the digits in the "word".

E.g Is your number in the set $\{8, 9, 10, 11, 12, 13, 14, 15\}$?

$0 \rightarrow 0000$	$8 \rightarrow 1000$
$1 \rightarrow 0001$	$9 \rightarrow 1001$
$2 \rightarrow 0010$	$10 \rightarrow 1010$
$3 \rightarrow 0011$	$11 \rightarrow 1011$
$4 \rightarrow 0100$	$12 \rightarrow 1100$
$5 \rightarrow 0101$	$13 \rightarrow 1101$
$6 \rightarrow 0110$	$14 \rightarrow 1110$
$7 \rightarrow 0111$	$15 \rightarrow 1111$

Ok so perhaps that wasn't so spectacular.

Now i'm going to allow you to lie once!

I'll tell you the question you lied on AND your number.

Ok so perhaps that wasn't so spectacular.

Now i'm going to allow you to lie once!

I'll tell you the question you lied on AND your number.

Ok so perhaps that wasn't so spectacular.

Now i'm going to allow you to lie once!

I'll tell you the question you lied on AND your number.

1. Is your number in the set $\{8, 9, 10, 11, 12, 13, 14, 15\}$?
2. Is your number in the set $\{4, 5, 6, 7, 12, 13, 14, 15\}$?
3. Is your number in the set $\{2, 3, 6, 7, 10, 11, 14, 15\}$?
4. Is your number in the set $\{1, 3, 5, 7, 9, 11, 13, 15\}$?
5. Is your number in the set $\{1, 2, 4, 7, 9, 10, 12, 15\}$?
6. Is your number in the set $\{1, 2, 5, 6, 8, 11, 12, 15\}$?
7. Is your number in the set $\{1, 3, 4, 6, 8, 10, 13, 15\}$?

1. Is your number in the set $\{8, 9, 10, 11, 12, 13, 14, 15\}$?
2. Is your number in the set $\{4, 5, 6, 7, 12, 13, 14, 15\}$?
3. Is your number in the set $\{2, 3, 6, 7, 10, 11, 14, 15\}$?
4. Is your number in the set $\{1, 3, 5, 7, 9, 11, 13, 15\}$?
5. Is your number in the set $\{1, 2, 4, 7, 9, 10, 12, 15\}$?
6. Is your number in the set $\{1, 2, 5, 6, 8, 11, 12, 15\}$?
7. Is your number in the set $\{1, 3, 4, 6, 8, 10, 13, 15\}$?

1. Is your number in the set $\{8, 9, 10, 11, 12, 13, 14, 15\}$?
2. Is your number in the set $\{4, 5, 6, 7, 12, 13, 14, 15\}$?
3. Is your number in the set $\{2, 3, 6, 7, 10, 11, 14, 15\}$?
4. Is your number in the set $\{1, 3, 5, 7, 9, 11, 13, 15\}$?
5. Is your number in the set $\{1, 2, 4, 7, 9, 10, 12, 15\}$?
6. Is your number in the set $\{1, 2, 5, 6, 8, 11, 12, 15\}$?
7. Is your number in the set $\{1, 3, 4, 6, 8, 10, 13, 15\}$?

1. Is your number in the set $\{8, 9, 10, 11, 12, 13, 14, 15\}$?
2. Is your number in the set $\{4, 5, 6, 7, 12, 13, 14, 15\}$?
3. Is your number in the set $\{2, 3, 6, 7, 10, 11, 14, 15\}$?
4. Is your number in the set $\{1, 3, 5, 7, 9, 11, 13, 15\}$?
5. Is your number in the set $\{1, 2, 4, 7, 9, 10, 12, 15\}$?
6. Is your number in the set $\{1, 2, 5, 6, 8, 11, 12, 15\}$?
7. Is your number in the set $\{1, 3, 4, 6, 8, 10, 13, 15\}$?

1. Is your number in the set $\{8, 9, 10, 11, 12, 13, 14, 15\}$?
2. Is your number in the set $\{4, 5, 6, 7, 12, 13, 14, 15\}$?
3. Is your number in the set $\{2, 3, 6, 7, 10, 11, 14, 15\}$?
4. Is your number in the set $\{1, 3, 5, 7, 9, 11, 13, 15\}$?
5. Is your number in the set $\{1, 2, 4, 7, 9, 10, 12, 15\}$?
6. Is your number in the set $\{1, 2, 5, 6, 8, 11, 12, 15\}$?
7. Is your number in the set $\{1, 3, 4, 6, 8, 10, 13, 15\}$?

1. Is your number in the set $\{8, 9, 10, 11, 12, 13, 14, 15\}$?
2. Is your number in the set $\{4, 5, 6, 7, 12, 13, 14, 15\}$?
3. Is your number in the set $\{2, 3, 6, 7, 10, 11, 14, 15\}$?
4. Is your number in the set $\{1, 3, 5, 7, 9, 11, 13, 15\}$?
5. Is your number in the set $\{1, 2, 4, 7, 9, 10, 12, 15\}$?
6. Is your number in the set $\{1, 2, 5, 6, 8, 11, 12, 15\}$?
7. Is your number in the set $\{1, 3, 4, 6, 8, 10, 13, 15\}$?

1. Is your number in the set $\{8, 9, 10, 11, 12, 13, 14, 15\}$?
2. Is your number in the set $\{4, 5, 6, 7, 12, 13, 14, 15\}$?
3. Is your number in the set $\{2, 3, 6, 7, 10, 11, 14, 15\}$?
4. Is your number in the set $\{1, 3, 5, 7, 9, 11, 13, 15\}$?
5. Is your number in the set $\{1, 2, 4, 7, 9, 10, 12, 15\}$?
6. Is your number in the set $\{1, 2, 5, 6, 8, 11, 12, 15\}$?
7. Is your number in the set $\{1, 3, 4, 6, 8, 10, 13, 15\}$?

Outline of talk

A code is just a set C of words of a fixed length n using fixed set of symbols F (called an alphabet).

Today: $F = \{0, 1\}$, natural for computers!

Example

The set $C = \{01001, 11011, 00010, 01011\}$ has length 5 and 4 words.

A code is just a set C of words of a fixed length n using fixed set of symbols F (called an alphabet).

Today: $F = \{0, 1\}$, natural for computers!

Example

The set $C = \{01001, 11011, 00010, 01011\}$ has length 5 and 4 words.

A code is just a set C of words of a fixed length n using fixed set of symbols F (called an alphabet).

Today: $F = \{0, 1\}$, natural for computers!

Example

The set $C = \{01001, 11011, 00010, 01011\}$ has length 5 and 4 words.

Some codes are great at detecting/correcting errors.

Example

The code $C = \{000...0, 111...1\}$ of length n is called the repetition code.

It can detect $n-1$ errors since 000...0 and 111...1 differ in n places.

It can correct $\lfloor \frac{n-1}{2} \rfloor$ errors since changing under half of the word still allows us to uniquely determine the message.

Some codes are great at detecting/correcting errors.

Example

The code $C = \{000...0, 111...1\}$ of length n is called the repetition code.

It can detect $n-1$ errors since 000...0 and 111...1 differ in n places.

It can correct $\lfloor \frac{n-1}{2} \rfloor$ errors since changing under half of the word still allows us to uniquely determine the message.

Some codes are great at detecting/correcting errors.

Example

The code $C = \{000...0, 111...1\}$ of length n is called the repetition code.

It can detect $n - 1$ errors since 000...0 and 111...1 differ in n places.

It can correct $\lfloor \frac{n-1}{2} \rfloor$ errors since changing under half of the word still allows us to uniquely determine the message.

Some codes are great at detecting/correcting errors.

Example

The code $C = \{000...0, 111...1\}$ of length n is called the repetition code.

It can detect $n-1$ errors since 000...0 and 111...1 differ in n places.

It can correct $\lfloor \frac{n-1}{2} \rfloor$ errors since changing under half of the word still allows us to uniquely determine the message.

Theorem

In general suppose all words in C differ in at least d places. Then C can detect $d-1$ errors and correct $\lfloor \frac{d-1}{2} \rfloor$ errors.

For example if:

$$C = \{01100, 10011, 11111\}$$

then 10011 and 11111 differ in 2 places and this is the best so $d = 2$. So this code can detect 1 error and correct 0 errors.

We can arrange to detect/correct ANY number of errors by using repetition codes. Why are we not done?

The repetition codes are inefficient. To guarantee accuracy we are sending very large words to encode only two piece of info!

We can arrange to detect/correct ANY number of errors by using repetition codes. Why are we not done?

The repetition codes are inefficient. To guarantee accuracy we are sending very large words to encode only two piece of info!

The rate of a code C of length n is the quantity $\frac{\log_2(|C|)}{n}$.

The smaller the rate the more inefficient the code is. For example the repetition code of length n has rate $\frac{1}{n}$ (which is very small if n is large).

Codes with high rate are likely not to detect/correct many errors. Coding theory is often about searching for codes with a good balance.

The rate of a code C of length n is the quantity $\frac{\log_2(|C|)}{n}$.

The smaller the rate the more inefficient the code is. For example the repetition code of length n has rate $\frac{1}{n}$ (which is very small if n is large).

Codes with high rate are likely not to detect/correct many errors. Coding theory is often about searching for codes with a good balance.

The rate of a code C of length n is the quantity $\frac{\log_2(|C|)}{n}$.

The smaller the rate the more inefficient the code is. For example the repetition code of length n has rate $\frac{1}{n}$ (which is very small if n is large).

Codes with high rate are likely not to detect/correct many errors. Coding theory is often about searching for codes with a good balance.

Outline of talk

So how did the trick work?

We encode our numbers 0 – 15 using an efficient code of length 7, called the Hamming code.

It can correct 1 error, hence the ability to tell up to one lie!

So how did the trick work?

We encode our numbers $0 - 15$ using an efficient code of length 7, called the Hamming code.

It can correct 1 error, hence the ability to tell up to one lie!

So how did the trick work?

We encode our numbers $0 - 15$ using an efficient code of length 7, called the Hamming code.

It can correct 1 error, hence the ability to tell up to one lie!

Encode as follows (the seven questions give the digits in a word):

$0 \to 0000000$	$8 \to 1000011$
$1 \to 0001111$	$9 \to 1001100$
$2 \to 0010110$	$10 \to 1010101$
$3 \to 0011001$	$11 \to 1011010$
$4 \to 0100101$	$12 \to 1100110$
$5 \to 0101010$	$13 \to 1101001$
$6 \to 0110011$	$14 \to 1110000$
$7 \to 0111100$	$15 \to 1111111$

We can still read off the number in binary:

0 → 0000000	8 → 1000011
1 → 0001111	9 → 1001100
2 → 0010110	10 → 1010101
3 → 0011001	11 → 1011010
4 → 0100101	12 → 1100110
5 → 0101010	13 → 1101001
6 → 0110011	14 → 1110000
7 → 0111100	15 → 1111111

The Hamming code has an interesting decoding algorithm!

Suppose $a_1 a_2 ... a_7$ is the result of at most one error.

Compute (assuming $1 + 1 = 0$):

$$
\begin{aligned}
a &= a_4 + a_5 + a_6 + a_7 \\
b &= a_2 + a_3 + a_6 + a_7 \\
c &= a_1 + a_3 + a_5 + a_7
\end{aligned}
$$

If $(a, b, c) = (0, 0, 0)$ then no error occurred, otherwise (a, b, c) describes the position of the error in binary.

E.g. Suppose your number was 12 and you lied on question 6.

1. Is your number in the set $\{8, 9, 10, 11, 12, 13, 14, 15\}$?
2. Is your number in the set $\{4, 5, 6, 7, 12, 13, 14, 15\}$?
3. Is your number in the set $\{2, 3, 6, 7, 10, 11, 14, 15\}$?
4. Is your number in the set $\{1, 3, 5, 7, 9, 11, 13, 15\}$?
5. Is your number in the set $\{1, 2, 4, 7, 9, 10, 12, 15\}$?
6. Is your number in the set $\{1, 2, 5, 6, 8, 11, 12, 15\}$?
7. Is your number in the set $\{1, 3, 4, 6, 8, 10, 13, 15\}$?

I receive the word 1100100.

E.g. Suppose your number was 12 and you lied on question 6.

1. Is your number in the set $\{8, 9, 10, 11, 12, 13, 14, 15\}$?
2. Is your number in the set $\{4, 5, 6, 7, 12, 13, 14, 15\}$?
3. Is your number in the set $\{2, 3, 6, 7, 10, 11, 14, 15\}$?
4. Is your number in the set $\{1, 3, 5, 7, 9, 11, 13, 15\}$?
5. Is your number in the set $\{1, 2, 4, 7, 9, 10, 12, 15\}$?
6. Is your number in the set $\{1, 2, 5, 6, 8, 11, 12, 15\}$?
7. Is your number in the set $\{1, 3, 4, 6, 8, 10, 13, 15\}$?

I receive the word 1100100.

1100100

$$a = 0 + 1 + 0 + 0 = 1$$
$$b = 1 + 0 + 0 + 0 = 1$$
$$c = 1 + 0 + 1 + 0 = 0$$

Since 110 is the number 6 in binary you lied on Q6.

Correcting gives 1100110 and so your number is 1100 in decimal, i.e. 12.

1100100

$$a = 0 + 1 + 0 + 0 = 1$$
$$b = 1 + 0 + 0 + 0 = 1$$
$$c = 1 + 0 + 1 + 0 = 0$$

Since 110 is the number 6 in binary you lied on Q6.

Correcting gives 1100110 and so your number is 1100 in decimal, i.e. 12.

Thanks for listening! Any questions?