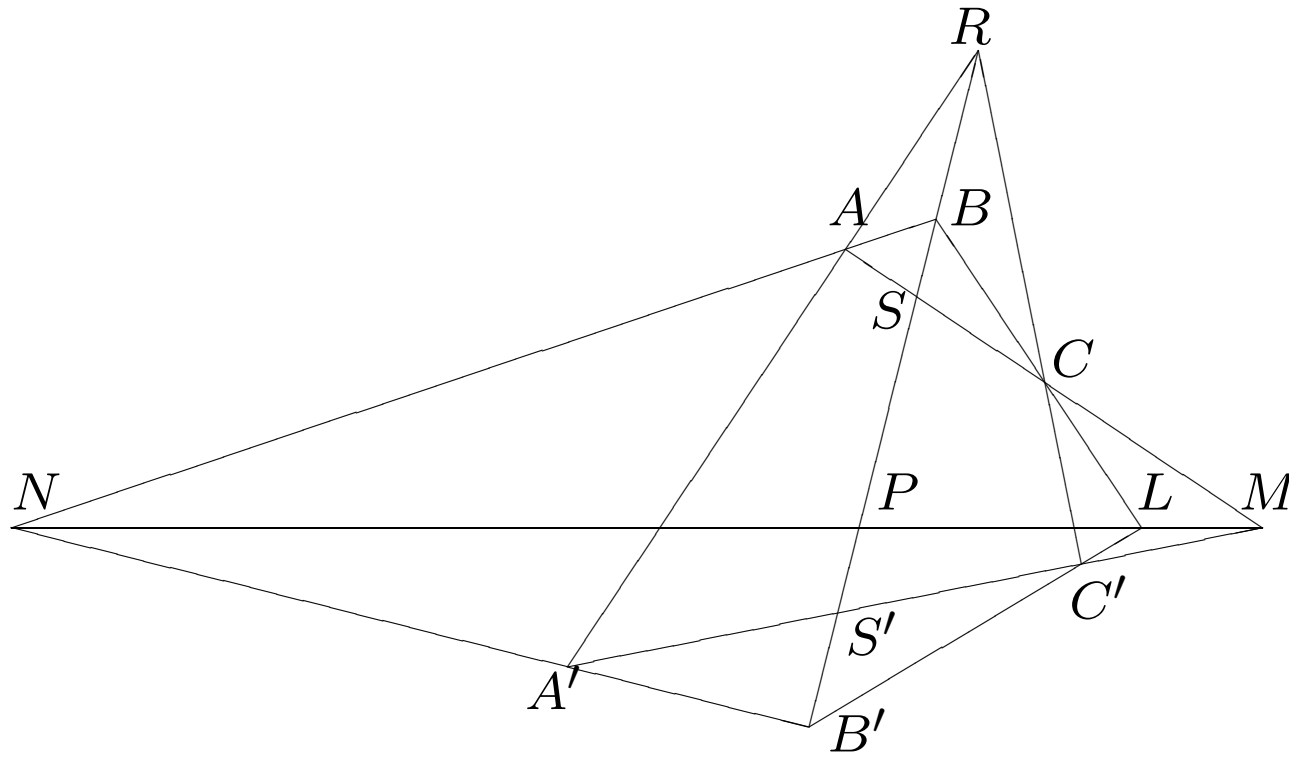


Something to look at!



## Desargues' Theorem

$$1 + 1 = 0$$

Seven executives in charge of seven units:

1. every two members of the executive were on a team together;
2. every two teams had a member in common.

Can this be done?

## A Biography of Gino Fano (1871-1952)

### Gino Fano

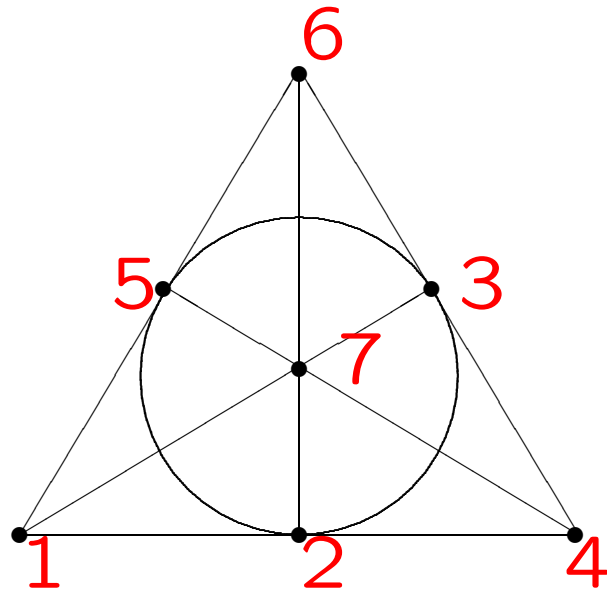
Born: 5 Jan 1871 in Mantua

Died: 8 Nov 1952 in Verona

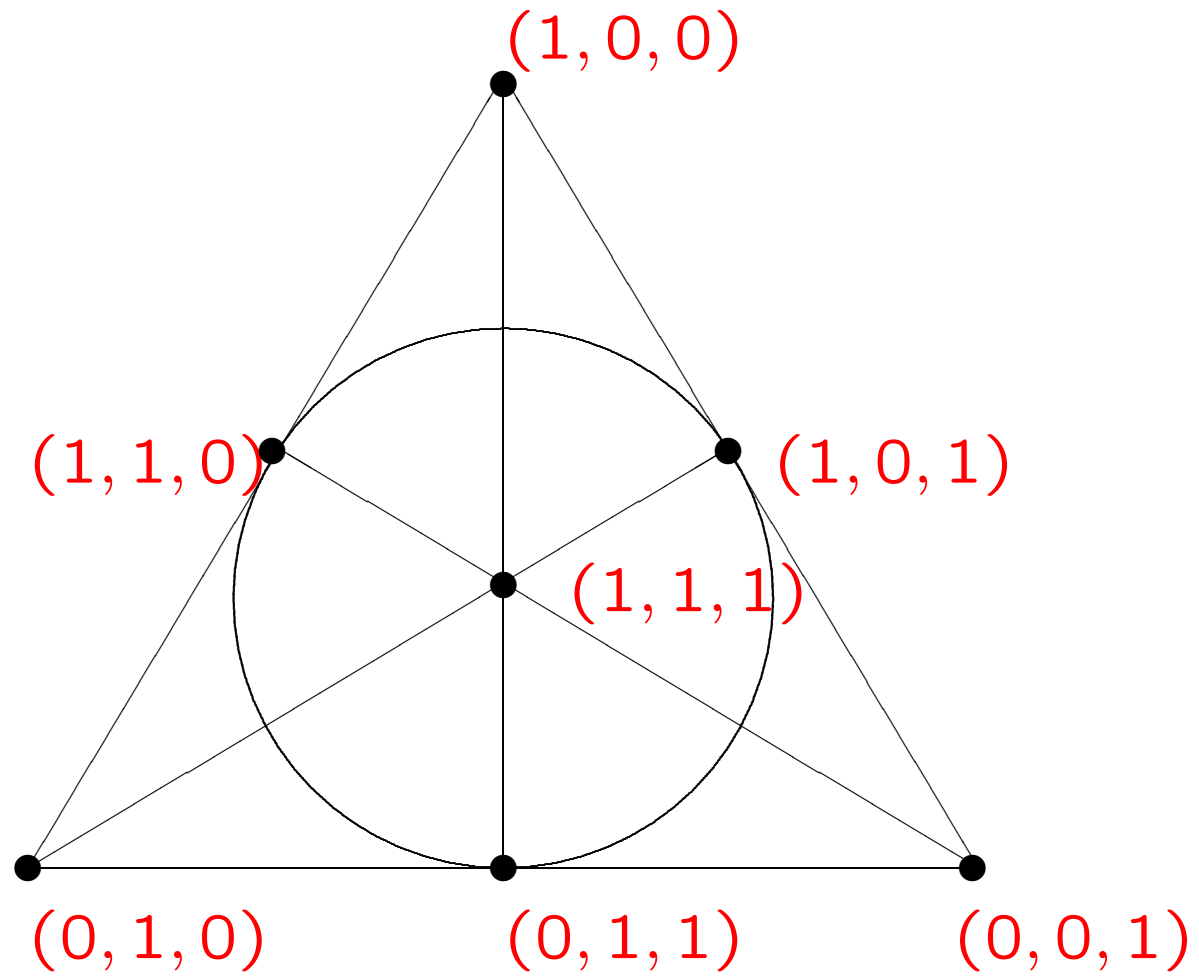
**Gino Fano** studied at Turin under Corrado Segre and met Guido Castelnuovo there. Then he went to Göttingen where he met Felix Klein. Fano became Castelnuovo's assistant, then was professor at Turin until he was deprived of his chair by the Fascist Regime in 1938. Fano then went to Switzerland and, after 1946, he taught in the USA and Italy.

His work was mainly on projective and algebraic geometry. Fano was a pioneer in finite geometry and one of the first people to try to set geometry on an abstract footing. Fano said the following:

*As a basis for our study we assume an arbitrary collection of entities of an arbitrary nature, entities which, for brevity, we shall call points, and this quite independently of their nature.*



1	2	3	4	5	6	7
2	3	4	5	6	7	1
4	5	6	7	1	2	3



The projective plane of order 2

Amazingly, the University decided to enlarge its executive committee to 13 as well its academic and administrative units. So, could they divide themselves into teams so that again

1. every two members of the executive were on a team together;
2. every two teams had a member in common.

Can this be done?

Answer: Yes it can!

1	2	3	4	5	6	7	8	9	10	11	12	13
2	3	4	5	6	7	8	9	10	11	12	13	1
4	5	6	7	8	9	10	11	12	13	1	2	3
10	11	12	13	1	2	3	4	5	6	7	8	9

$$7 = 2^2 + 2 + 1, \quad 13 = 3^2 + 3 + 1.$$

# Information Theory

## CODING THEORY

*correct messages*

CD players  
disk drives  
photographs  
digital radio

## CRYPTOGRAPHY

*secret messages*

electronic authentication  
banking  
credit cards  
military communications

# **A Mathematical Theory of Communication**

By C. E. Shannon

*The fundamental problem of communication is that of reproducing at one point either exactly or approximately a message selected at another point.*

The Bell System Technical Journal **27** (1948), 379–423, 623–656.

Think of a whole number between 0 and 15.

Answer the following seven questions: *you are allowed to answer any one, but only one, of the questions incorrectly.*

1. Is it 8 or greater ?
2. Is it one of 4, 5, 6, 7, 12, 13, 14, 15 ?
3. Is it one of 2, 3, 6, 7, 10, 11, 14, 15 ?
4. Is it odd ?
5. Is it one of 1, 2, 5, 6, 8, 11, 12, 15 ?
6. Is it one of 2, 3, 4, 5, 8, 9, 14, 15 ?
7. Is it one of 1, 2, 4, 7, 9, 10, 12, 15 ?

## The essential idea

YES = 1, NO = 0.

Send 1, receive 0.

An error is not detected.

Add redundancy:

YES = 11, NO = 00.

Suppose 01 is received.

Then either 00 or 11 was sent.

So an error has been detected but not corrected.

Add more redundancy:

YES = 111, NO = 000.

Suppose 101 is received.

Then, the correct message is 111 = YES,

under the assumption of at most one error.

All triples:

000, 001, 010, 011, 100, 101, 110, 111

The code consisting of 000 and 111 is *perfect*: every triple has only one digit different from a codeword.

## Morse Code as used by the British Army

0 = .      1 = \_

A	01	N	10	0	1
B	1000	O	111	1	01
C	1010	P	0110	2	001
D	100	Q	1101	3	00011
E	0	R	010	4	00001
F	0010	S	000	5	0
G	110	T	1	6	1000
H	0000	U	001	7	11000
I	00	V	0001	8	100
J	0111	W	011	9	10
K	101	X	1001		
L	0100	Y	1011		
M	11	Z	1100		

To signal four directions, the shortest code is

$$C_1 = \left\{ \begin{array}{cccc} 00, & 01, & 10, & 11 \\ \text{N} & \text{E} & \text{W} & \text{S} \end{array} \right\} .$$

This code does not allow for errors; so add an extra digit, namely a *parity check*:

$$C_2 = \left\{ \begin{array}{cccc} 000, & 011, & 101, & 110 \\ \text{N} & \text{E} & \text{W} & \text{S} \end{array} \right\} .$$

This will *detect* an error.

Suppose 010 is received: **N**, **E**, **S** are all acceptable messages.

$$C_3 = \left\{ \begin{array}{cccc} 00000, & 01101, & 10110, & 11011 \\ \text{N} & \text{E} & \text{W} & \text{S} \end{array} \right\} .$$

Suppose 01100 is received. The number of digits different:

N	E	W	S
2	1	3	4

So 01100 is decoded as **E** = 01101.

The code  $C_3$  corrects one error!

$$C_3 = \{ \underset{\text{N}}{00000}, \underset{\text{E}}{01101}, \underset{\text{W}}{10110}, \underset{\text{S}}{11011} \} .$$

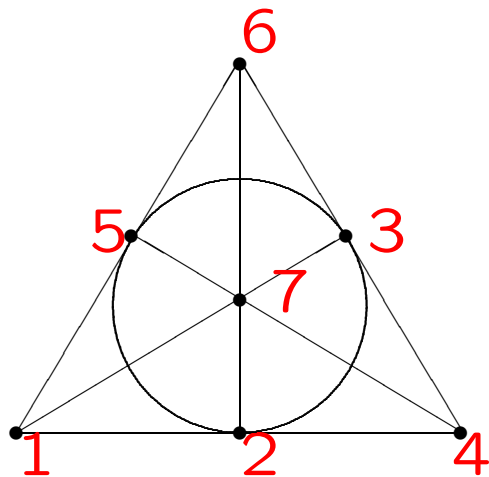
Every two codewords have either three or four digits different.

It is NOT perfect; for example, 11000 is not uniquely decoded !

The code  $C_3$  is called a  $[5, 2]$  or  $[5, 2, 3]$  code.

The numbers 0 to 15 in binary notation plus extra bits for error correction

0	0	0	0	0	0	0	0
1	0	0	0	1	1	0	1
2	0	0	1	0	1	1	1
3	0	0	1	1	0	1	0
4	0	1	0	0	0	1	1
5	0	1	0	1	1	1	0
6	0	1	1	0	1	0	0
7	0	1	1	1	0	0	1
8	1	0	0	0	1	1	0
9	1	0	0	1	0	1	1
10	1	0	1	0	0	0	1
11	1	0	1	1	1	0	0
12	1	1	0	0	1	0	1
13	1	1	0	1	0	0	0
14	1	1	1	0	0	1	0
15	1	1	1	1	1	1	1



	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0
13	1	1	0	1	0	0	0
6	0	1	1	0	1	0	0
3	0	0	1	1	0	1	0
1	0	0	0	1	1	0	1
8	1	0	0	0	1	1	0
4	0	1	0	0	0	1	1
10	1	0	1	0	0	0	1
2	0	0	1	0	1	1	1
9	1	0	0	1	0	1	1
12	1	1	0	0	1	0	1
14	1	1	1	0	0	1	0
7	0	1	1	1	0	0	1
11	1	0	1	1	1	0	0
5	0	1	0	1	1	1	0
15	1	1	1	1	1	1	1

A 1-error-correcting perfect code!

A non-binary code

0 747 55099 9

0 19 850295 8

0 521 59538 *X*

An ISBN is a 10-digit number

$$x_1 x_2 \dots x_{10}$$

where

- (i) each of the first 9 digits is one of  $0, 1, \dots, 9$ ;
- (ii) the last digit is one of  $0, 1, \dots, 9, X$ ;
- (iii)  $11$  divides  $x_1 + 2x_2 + \dots + 9x_9 + 10x_{10}$ .

	0	7	4	7	5	5	0	9	9	9
×	1	2	3	4	5	6	7	8	9	10
	0	3	1	6	3	-3	0	6	4	2

- (i) any unknown digit in a given position can be calculated;
- (ii) an interchange of two digits is detected.

Why? The number 11 is a prime!

$x$	1	2	3	4	5	6	7	8	9	10
$x^{-1}$	1	6	4	3	9	2	8	7	5	10

$$x_1 + 2x_2 + \dots + 9x_9 + 10x_{10} \equiv 0 \pmod{11};$$

$$x_{10} \equiv x_1 + 2x_2 + \dots + 9x_9 \pmod{11}.$$

Galileo used a [255, 233] code plus a convolutional code.

CD players use [32, 28] and [28, 24] codes interleaved to cope with burst errors.

Quantum codes for a quantum computer use the field of 4 elements:

$$\begin{aligned}\mathbf{F}_4 &= \{0, 1, \omega, \bar{\omega} \mid 1 + 1 = 0, \omega + \bar{\omega} = 1 = \omega\bar{\omega}\} \\ &\neq \mathbf{Z}_4 = \{0, 1, 2, 3 \mid 4 = 0\}.\end{aligned}$$

A classical quotation:

Jdoold hww rpqlv glylvd lq sduwhv wuhv

## Caesar's cipher

Plain	A	B	C	D	E	F	G	H	I	J	K	L	M
Cipher	D	E	F	G	H	I	J	K	L	M	N	O	P

Plain	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cipher	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

$$c \equiv p + 3 \pmod{26}, \quad 1 \leq c \leq 26$$

$$p \equiv c - 3 \pmod{26}, \quad 1 \leq p \leq 26$$

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Jdoold

J	d	o	o	l	d
10	4	15	15	12	4
7	1	12	12	9	1
G	a	l	l	i	a

Gallia

Jdoold hww rpqlv glylvd lq sduwhv wuhv

Gallia est omnis divisa in partes tres

Two principles for Caesar's cipher:

- (i) *Anyone who can encipher a message can also decipher it.*
- (ii) *Sender and receiver share a common secret key that must be transmitted before encryption can start.*

## Prime numbers

Primes: 2, 3, 5, 7, 11, 13, 17, 19, 23, ...

Non-primes: 4, 6, 8, 9, 10, 12, 14, 15, 16, ...

**Theorem** (Fermat) *If  $m$  is not a multiple of the prime  $p$ , then*

$$m^{p-1} \equiv 1 \pmod{p}.$$

**Example** Let  $m = 3$ ,  $p = 7$ . Then

$$3^{7-1} = 3^6 = (3^3)^2 = 27^2 \equiv (-1)^2 = 1.$$

**Theorem** (Fermat–Euler) *If  $m$  is not a multiple of either of the primes  $p$ ,  $q$ , then*

$$m^{(p-1)(q-1)} \equiv 1 \pmod{pq}.$$

## Public-key cryptography

- (1) There are PUBLIC keys  $e$  and  $n$  for enciphering.
- (2) There is a PRIVATE key  $d$  for deciphering.
- (3) Here,  $n = pq$ , where  $p$  and  $q$  are large primes.
- (4) 'Large' means around  $10^{50}$  digits!
- (5) Multiplication of two such numbers is quick, that is, a few milliseconds.
- (6) Factoring an  $n$  of about  $10^{100}$  digits into two large primes is currently computationally impossible!

## Rivest, Shamir, and Adleman (RSA)

(1) Ben wants to send a message  $M$  to Rachel.

(2) Rachel chooses  $e$  and  $n = pq$ , where  $p$  and  $q$  are primes such that  $(e, (p - 1)(q - 1)) = 1$ .

Here  $e$  and  $n = pq$  are PUBLIC, but  $p$  and  $q$  are not.

(3) Ben calculates  $M^e \pmod{n}$ , where  $0 < M < n$ .

(4) Rachel calculates  $d$  so that  $de \equiv 1 \pmod{(p - 1)(q - 1)}$

and then calculates  $(M^e)^d \equiv M \pmod{n}$ .

- (1) Rachel chooses  $e = 7$  and  $n = 33 = 3 \times 11$ .
- (2) Ben wants to send a message  $M = 19$  to Rachel.
- (3) Ben calculates  $M^e = 19^7 = 19^{4+2+1} \equiv 13 \pmod{33}$ ; this is transmitted.
- (4) Rachel calculates  $d = 3$  such that

$$de = 3 \times 7 = 21 \equiv 1 \pmod{20 = (3 - 1)(11 - 1)}$$

and then calculates

$$(M^e)^d = 13^3 = 169 \times 13 \equiv 4 \times 13 = 52 \equiv 19 = M \pmod{33}.$$