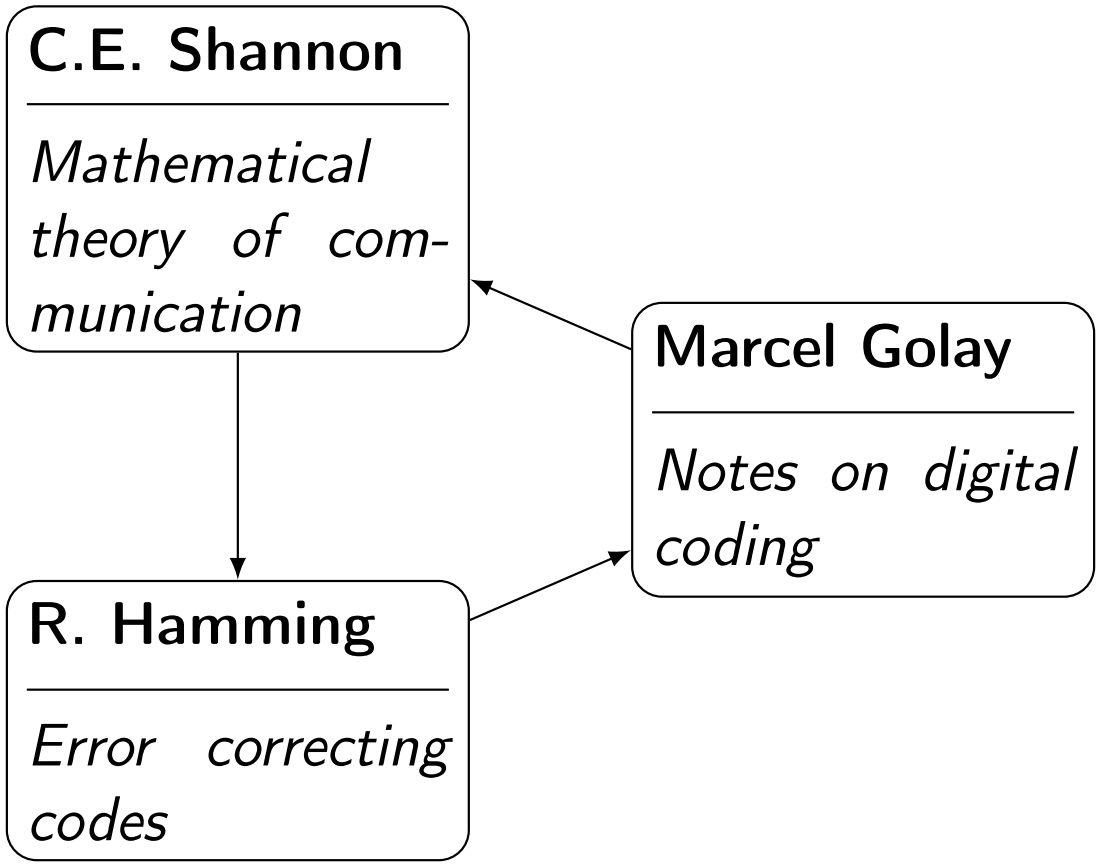
Théorie des codes

Alain Busser, Franck Jean-Albert

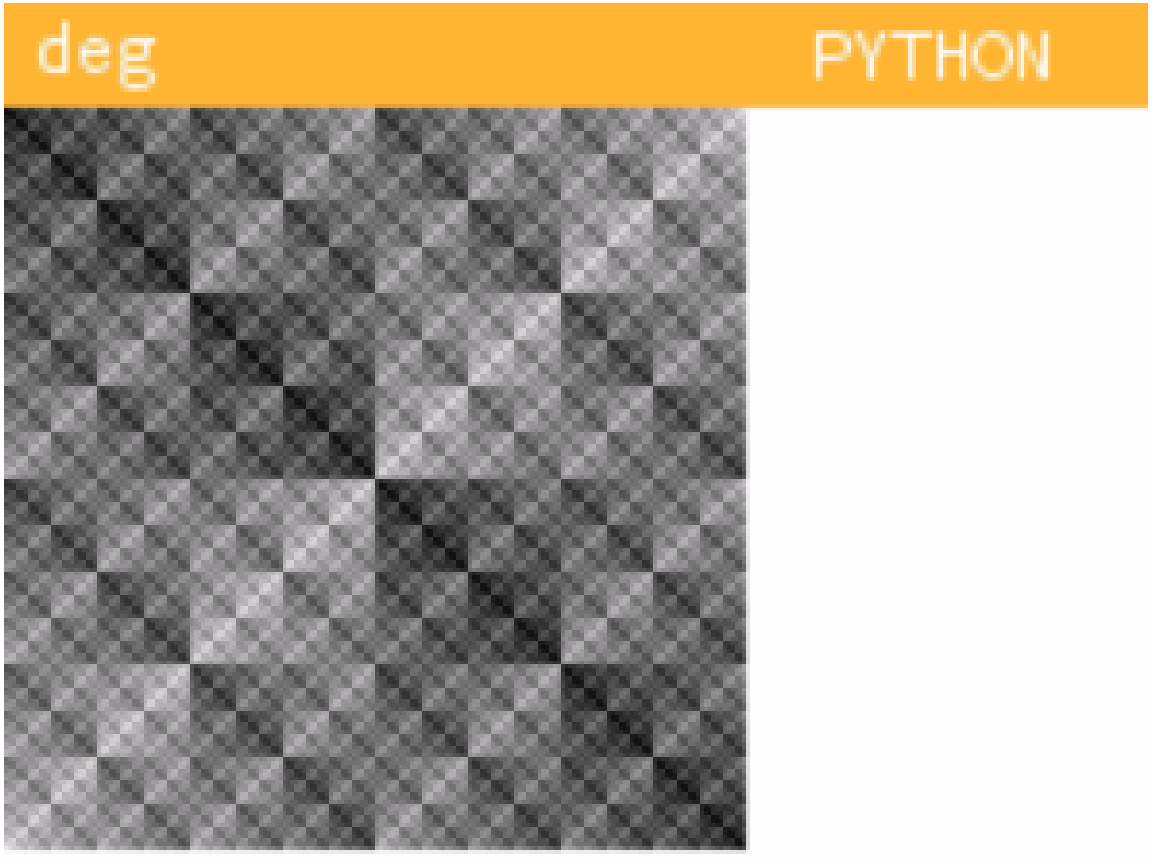
4 novembre 2020

1949
Shannon, Hamming et Golay

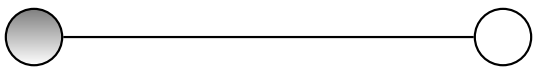


Distance de Hamming

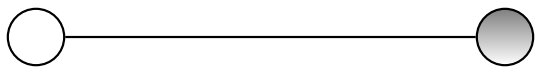
https://workshop.numworks.com/python/alain-busser/hamming

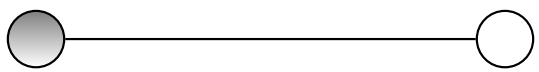


Dimension 1



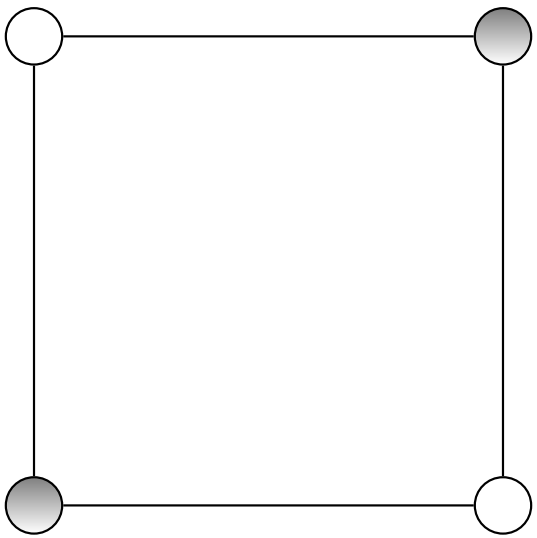
Dimension 2



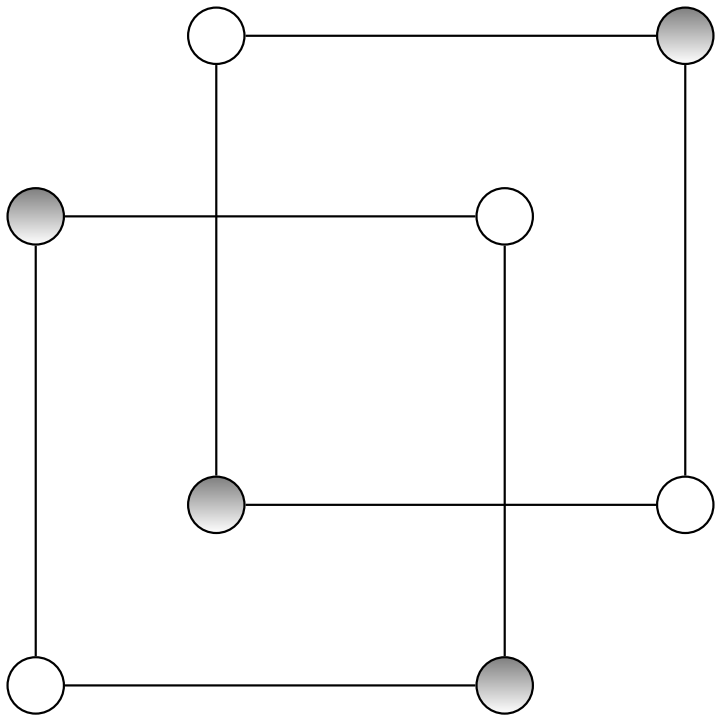


Dimension 2

(0,0) et (1,1) sont à distance 2

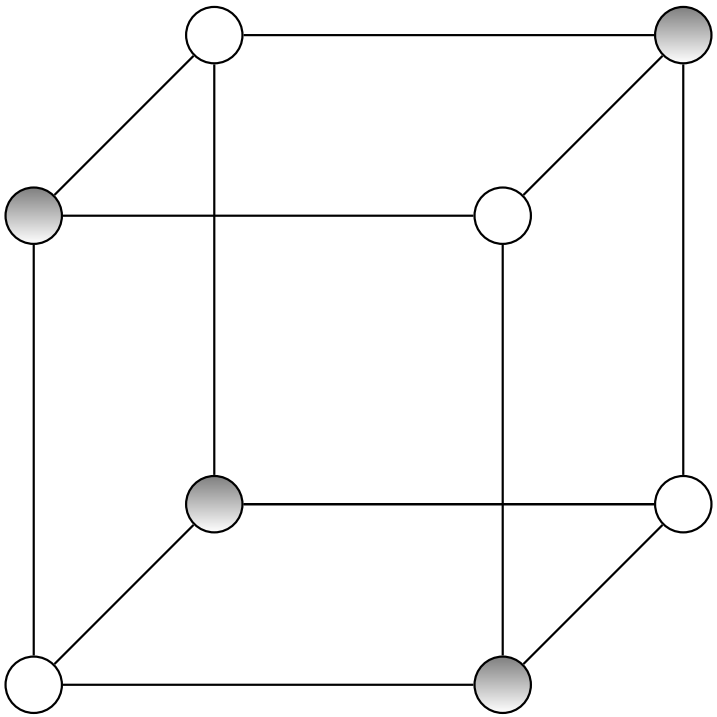


Dimension 3

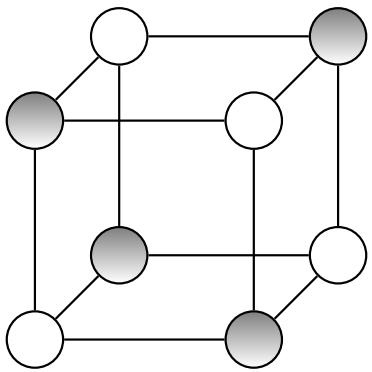


Dimension 3

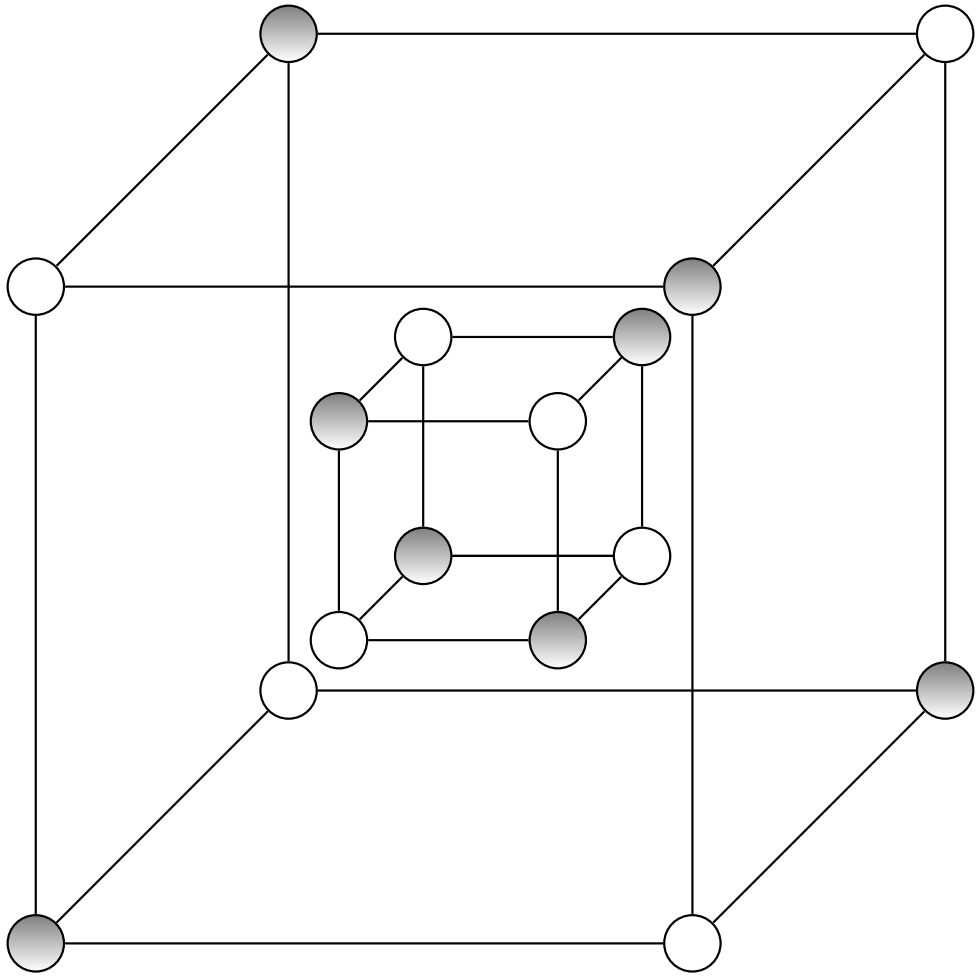
Les sommets du tétraèdre sont à distance mutuelle 2



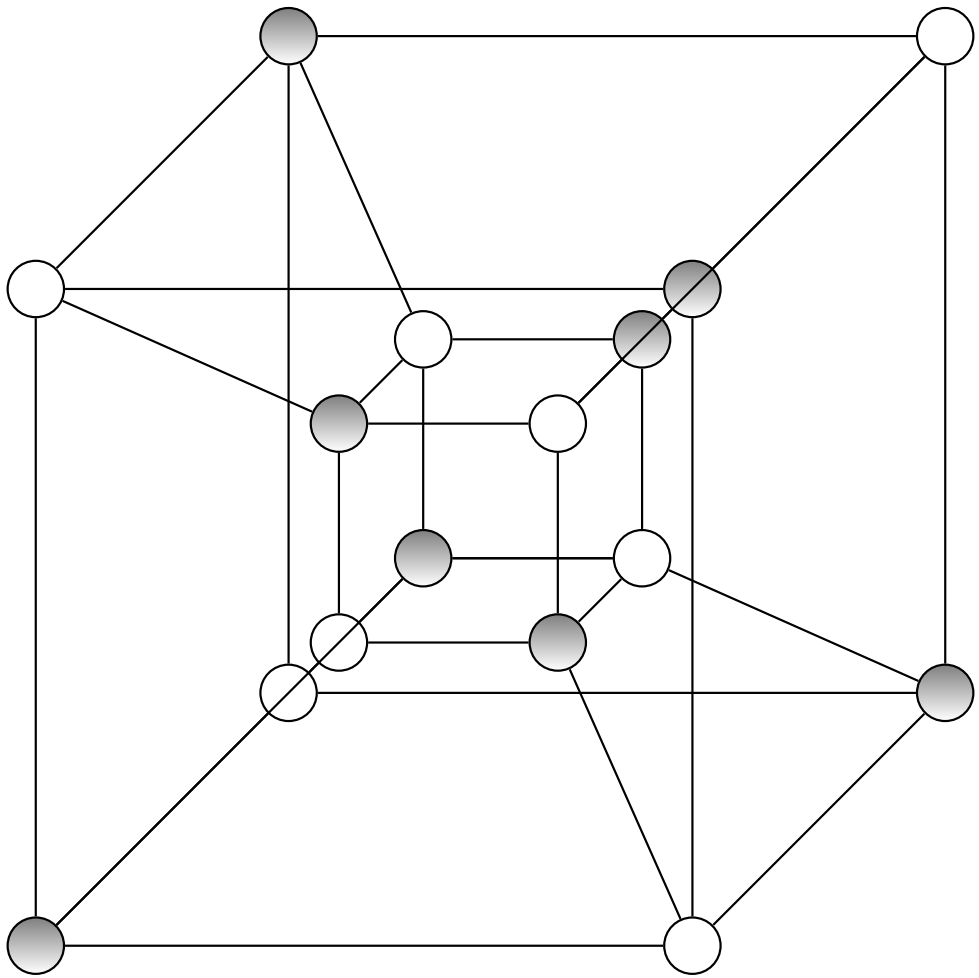
Dimension 4



Dimension 4



Dimension 4
Distance de Hamming 2



Code (4,3,2)

- $000 \mapsto 0000$
- $001 \mapsto 0011$
- $011 \mapsto 0110$
- $010 \mapsto 0101$
- $101 \mapsto 1010$
- $100 \mapsto 1001$
- $110 \mapsto 1100$
- $111 \mapsto 1111$

Code (4,3,2)

Matrice génératrice

$$\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix} \text{ ou } \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$$

La magie de Hamming

1	3
5	7
9	11
13	15

2	3
6	7
10	11
14	15

4	5
6	7
12	13
14	15

8	9
10	11
12	13
14	15

Code (7,4,3)

Matrice génératrice

$$\begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Code (7,4,3)

Matrice génératrice

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \text{ ou } \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}$$

Code (23,11,8)

Marcel Golay, 1949

$$\begin{pmatrix}
1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\
1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\
1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\
1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\
1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \\
1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\
1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\
1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\
1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\
1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\
0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1
\end{pmatrix}$$

Unicité du code de Golay

Marcel Golay 1949

A necessary but not sufficient condition [...] is the existence of three or more numbers of a line of Pascal's triangle which add up to an exact power of 2.

...					
1	21	210	1330	5985	...
1	22	231	1540	7315	...
1	**23**	**253**	**1771**	8855	...

$$1 + 23 + 253 + 1771 = 2048 = 2^{11}$$

Unicité du code de Golay

Marcel Golay 1949

A necessary but not sufficient condition [...] is the existence of three or more numbers of a line of Pascal's triangle which add up to an exact power of 2.

...

1	89	3916	113564	2441626	...
1	**90**	**4005**	117480	2555190	...

$$1 + 90 + 4005 = 4096 = 2^{12}$$

Unicité du code de Golay

Marcel Golay 1949

We should have $r + r(90 - r) = 2^{11}$, which is impossible for integer values of r.

$$r^2 - 91r + 2048 = 0$$

$$\Delta = 91^2 - 4 \times 2048 = 8281 - 2048 = 89$$

$$\frac{91 - \sqrt{89}}{2} \notin \mathbb{N} \wedge \frac{91 + \sqrt{89}}{2} \notin \mathbb{N}$$

Existence du code de Golay

Remarque :
L'équation $r + r(23 - r) = 2^7$ a deux solutions : 8 et 16.

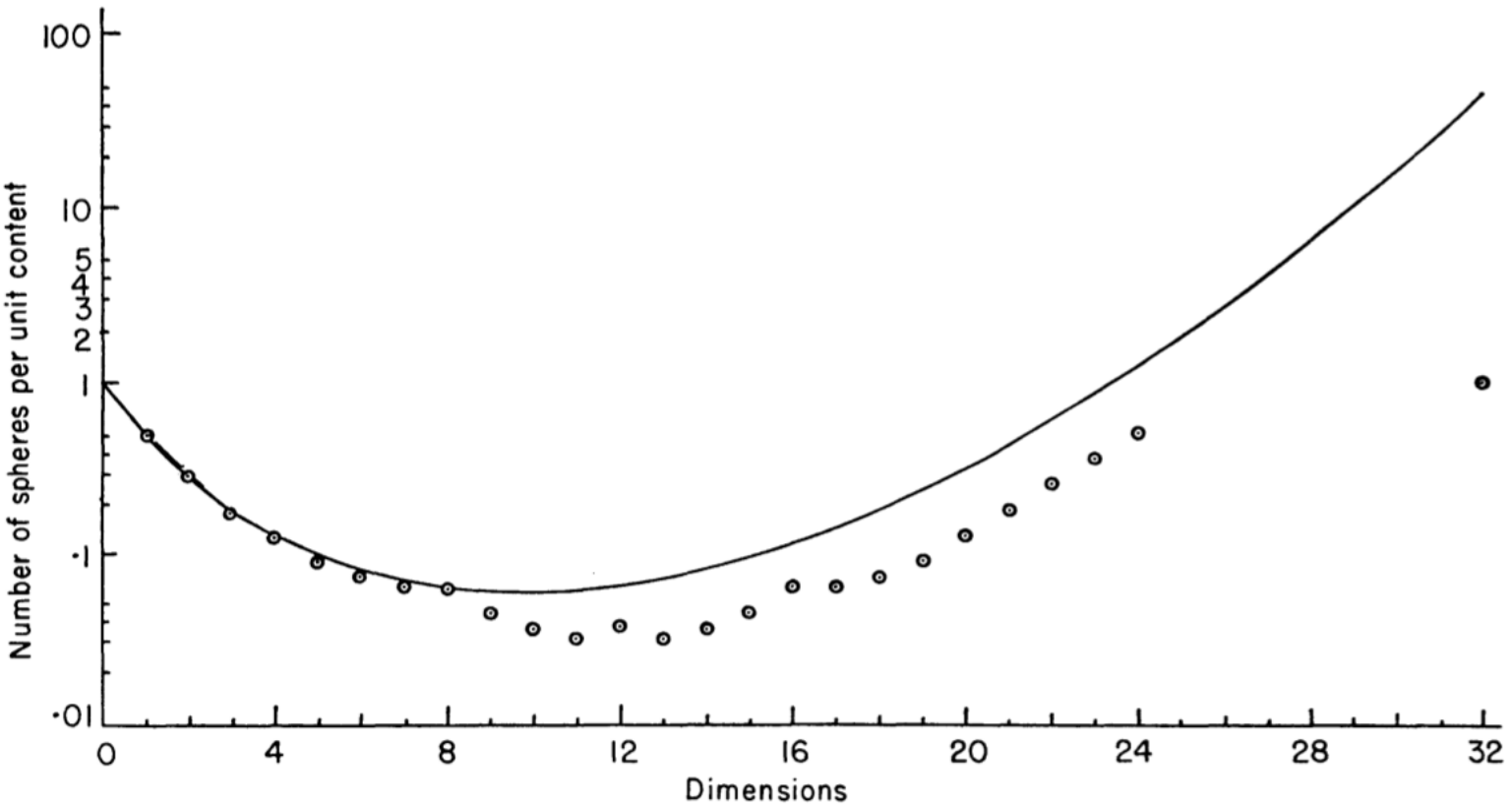
Groupes de Mathieu

http://brauer.maths.qmul.ac.uk/Atlas/v3/spor/M24/

Les symétries du code de Golay forment un groupe simple : le groupe de Mathieu M_{23}.
Les symétries du code de Golay étendu forment un autre groupe simple : Le groupe de Mathieu M_{24}.
Ces groupes sont sporadiques.

Réseaux en dimension supérieure

John Leech, 1965



Groupes de Conway

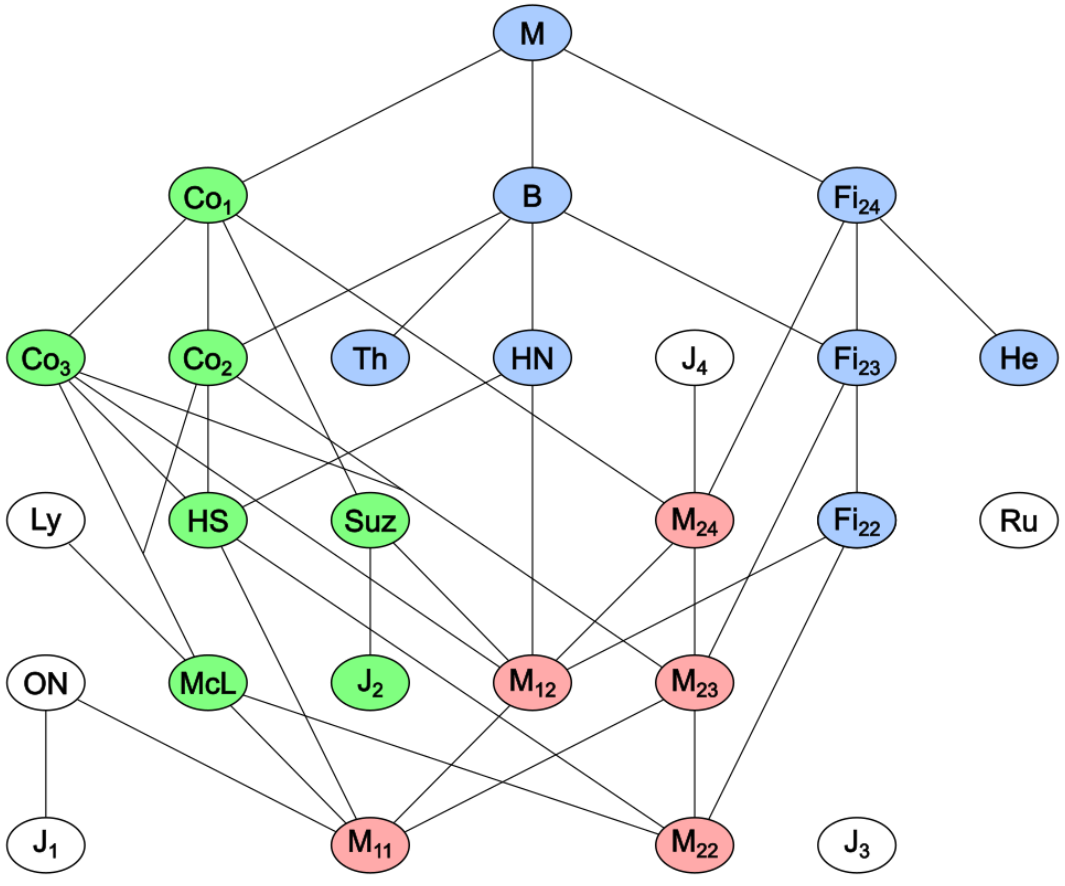
Théorème (Conway 1968)

Le quotient du groupe des automorphismes du réseau de Leech par son centre est un groupe simple.

Le groupe Co_1 de Conway contient 4 157 776 806 543 360 000 éléments. C'est un groupe sporadique.
Deux stabilisateurs inclus dans le groupe des automorphismes du réseau de Leech sont également des groupes simples sporadiques : les groupes de Conway Co_2 et Co_3.

Groupes sporadiques

Il n'y en a que 26



Monstrueux !

Comment Borcherds a eu la médaille Fields

Simon Norton (1952-2019) a construit le groupe de Harada-Norton[1]. Avec John Conway (1937-2020) il a établi des connexions entre le monstre de Fischer[2] et les formes modulaires. Remarque de John McKay (1939-) ayant valu une médaille Fields à Richard Borcherds (1959-) en 1998.

[1] et créé le jeu Snort

[2] construit par Conway à partir du réseau de Leech