

# L'erreur dans la transmission d'informations numériques, comment la corriger ?

Martino Borello  
(Paris 8 - LAGA)

20/10/2017



IL FAUT CANGER !



IL FAUT ~~X~~ANGER !



RANGER

CHANGER

MANGER

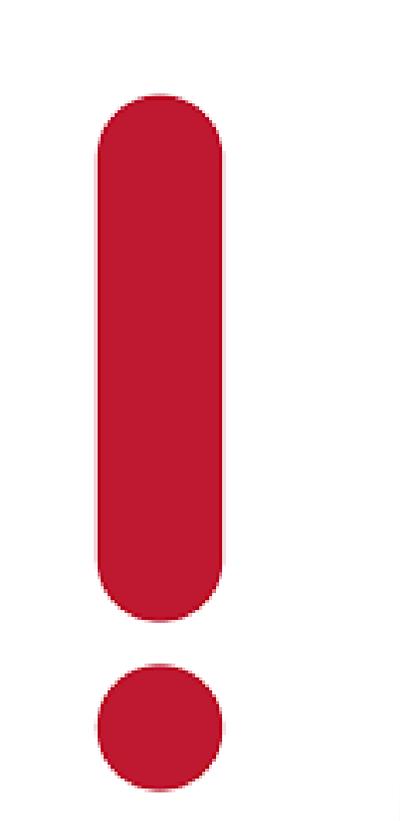


# Répéter

IL FAUT **C**ANGER !  
IL FAUT MANGER !



**M**MANGER



## Ajouter des informations

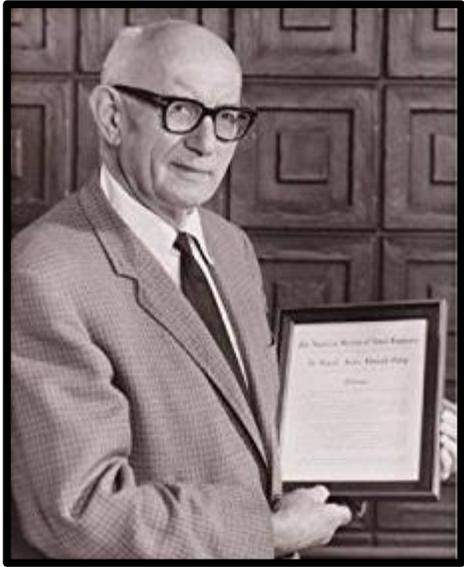
IL FAUT **C**ANGER  
UN BON GATEAU !



**M**ANGER



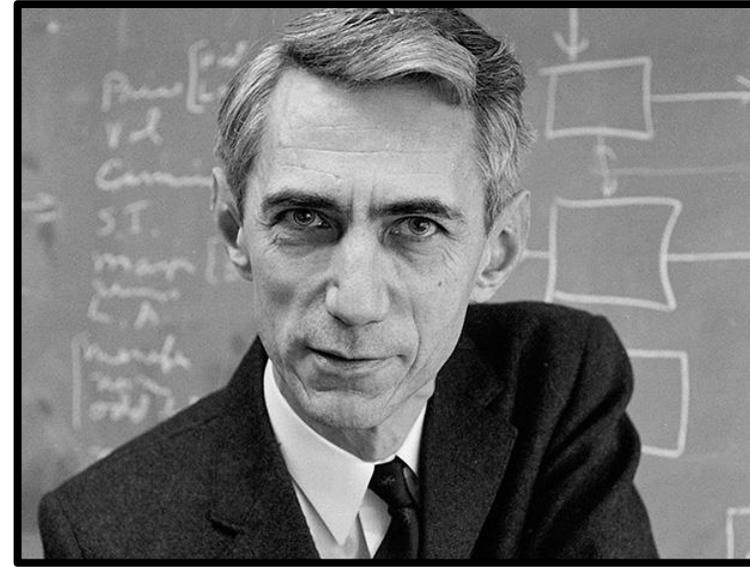
# Les pères fondateurs



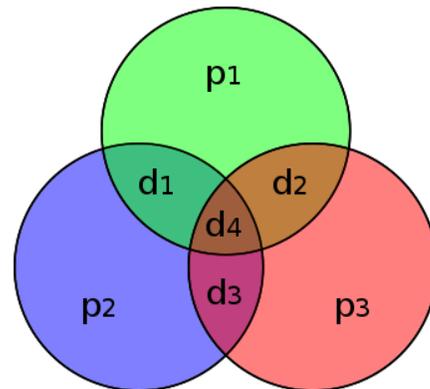
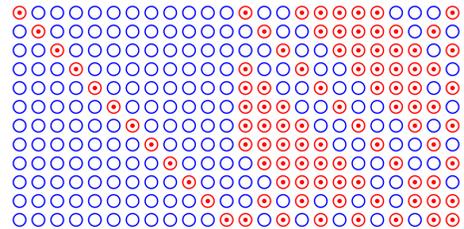
Marcel J. E. Golay  
1902-1989  
Suisse



Richard W. Hamming  
1915-1998  
États-Unis



Claude E. Shannon  
1916-2001  
États-Unis



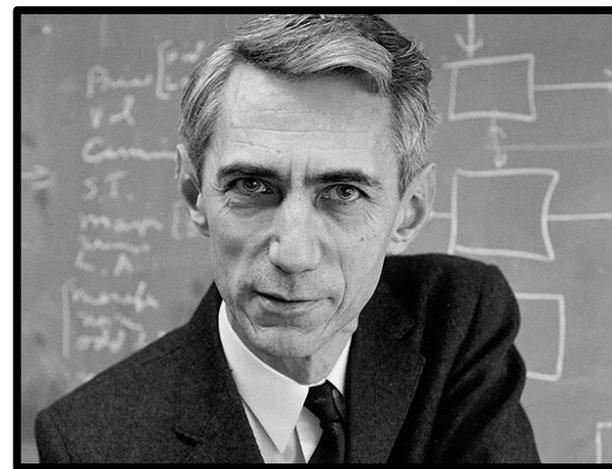
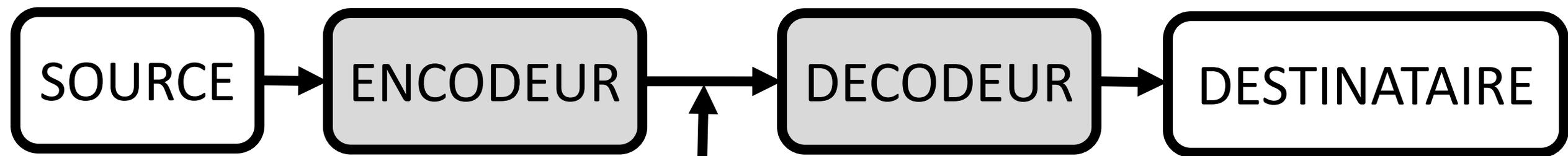
Reprinted with corrections from *The Bell System Technical Journal*,  
Vol. 27, pp. 379-423, 623-656, July, October, 1948.

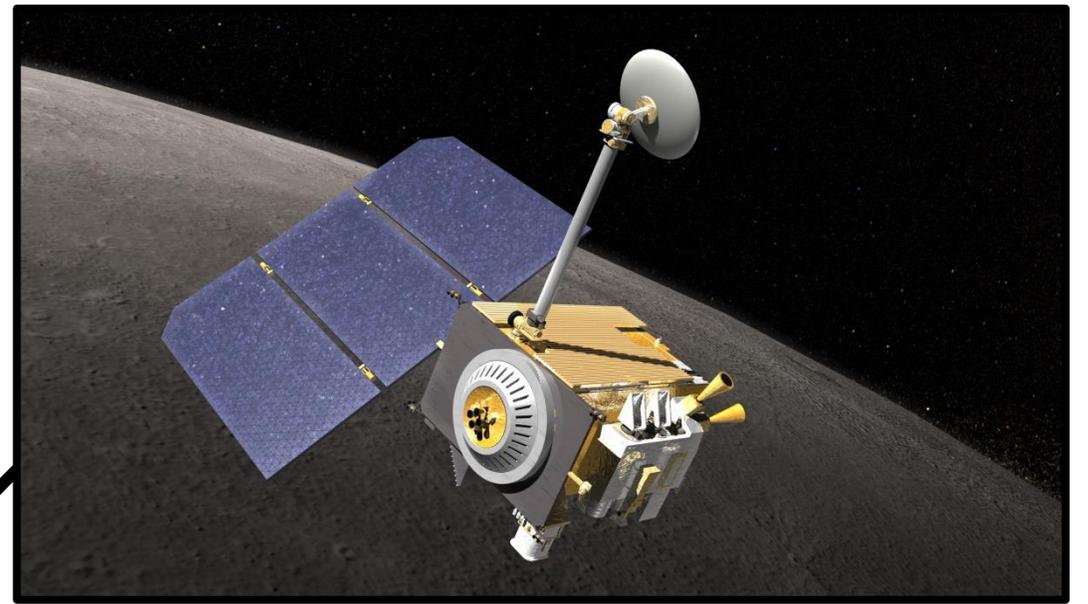
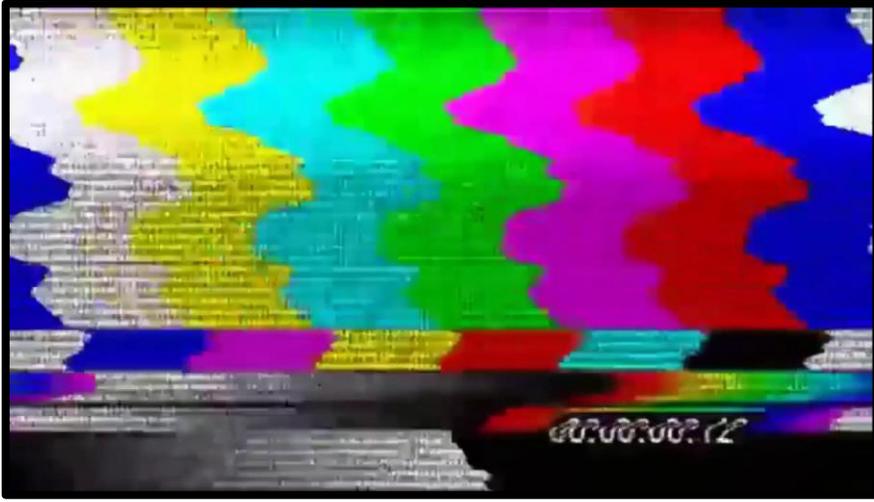
## A Mathematical Theory of Communication

By C. E. SHANNON

### INTRODUCTION

THE recent development of various methods of modulation such as PCM and PPM which have increased the bandwidth for signal-to-noise ratio has intensified the interest in a general theory of communication. A basis for such a theory is contained in the important papers of Nyquist<sup>1</sup> and Hartley<sup>2</sup> on this subject. In the present paper we will extend the theory to include a number of new factors, in particular the effect of noise in the channel, and the savings possible due to the statistical structure of the original message and the nature of the channel.

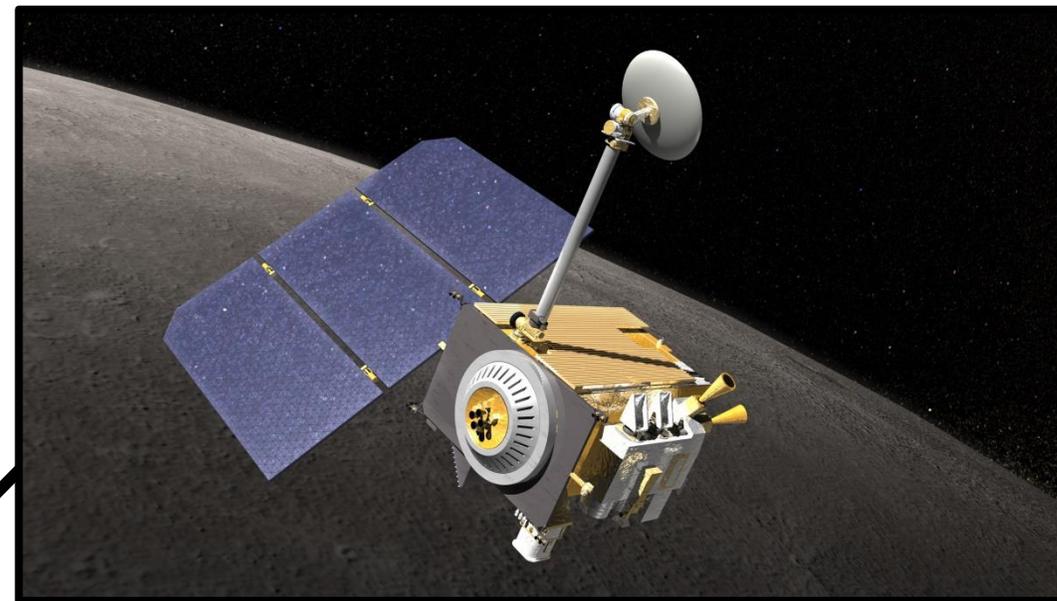
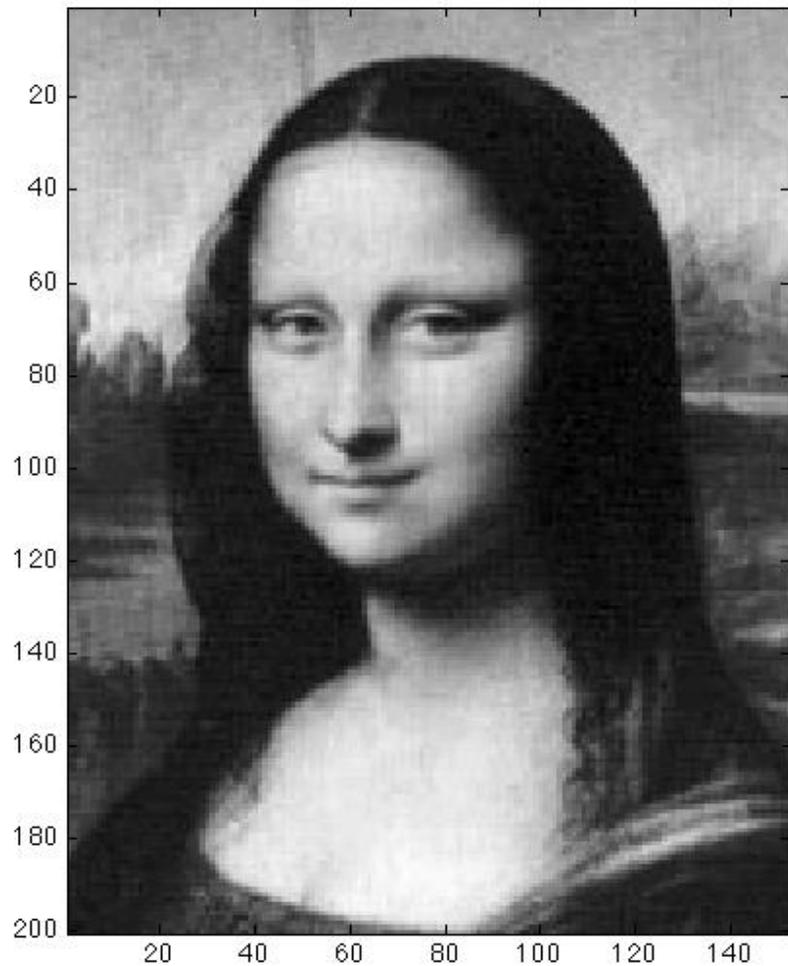




BRUIT



Image transmise de la terre

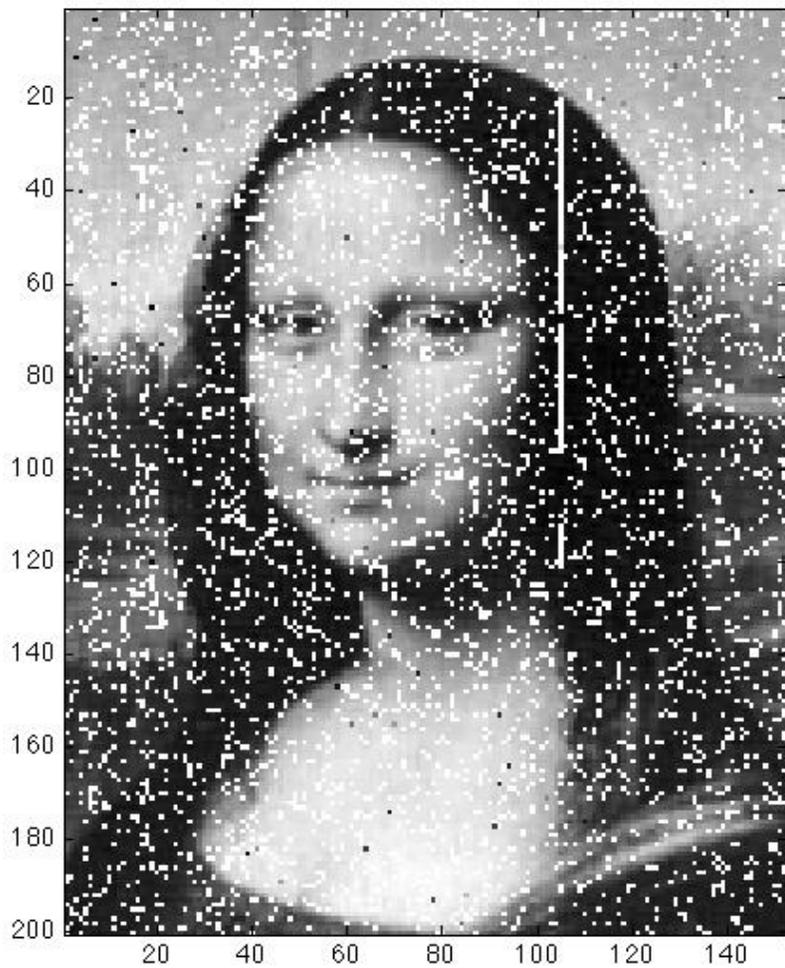


NASA's Lunar Reconnaissance Orbiter (LRO)

BRUIT



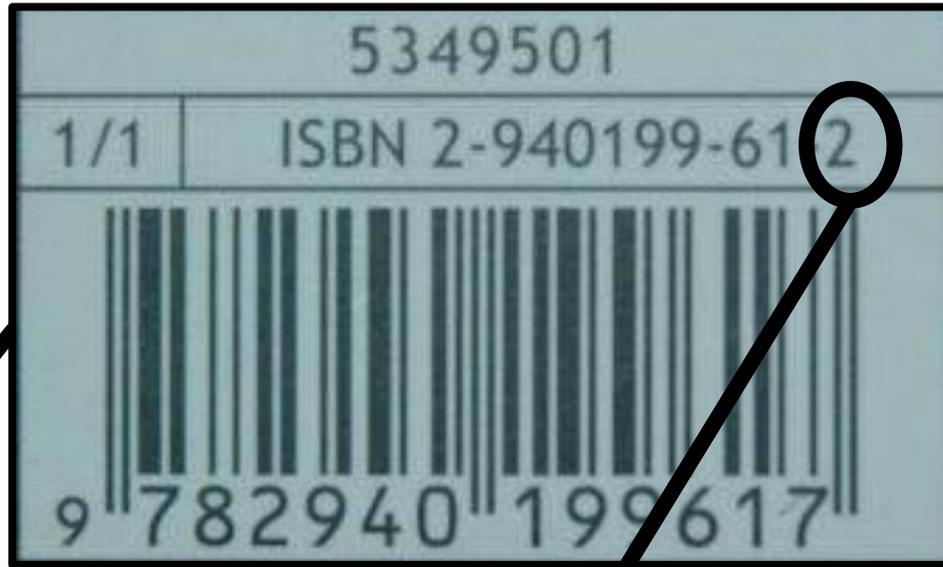
Image reçue (sans code)



NASA's Lunar Reconnaissance Orbiter (LRO)

BRUIT





$$\begin{aligned} 2 &= (2 \times 1 + 9 \times 2 + 4 \times 3 + 0 \times 4 + 1 \times 5 + 9 \times 6 + 9 \times 7 + 6 \times 8 + 1 \times 9) \bmod 11 \\ &= 211 \bmod 11 = (19 \times 11 + 2) \bmod 11 \end{aligned}$$

**Détecter**

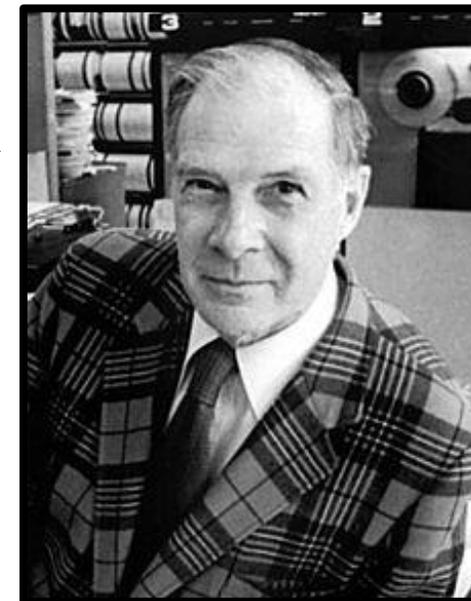


### Ordinateur **modèle V** :

- Il occupait environ 100 mètres carrés ;
- Il pesait 10 tonnes ;
- Il pouvait résoudre des systèmes de 13 équations linéaires en moins de 4 heures ;
- chaque fois que l'ordinateur découvrait une erreur dans l'entrée, il abandonnait simplement le travail et prenait le suivant.

**Deux week-ends de suite, je suis arrivé et j'ai trouvé qu'une erreur était survenue et rien n'avait été fait.**

**J'étais vraiment en colère et agacé parce que je voulais ces réponses et deux week-ends avaient été perdus. Et alors j'ai dit "Bon sang, si la machine peut détecter une erreur, pourquoi ne peut-elle pas localiser la position de l'erreur et la corriger ?"**



# ENCODEUR

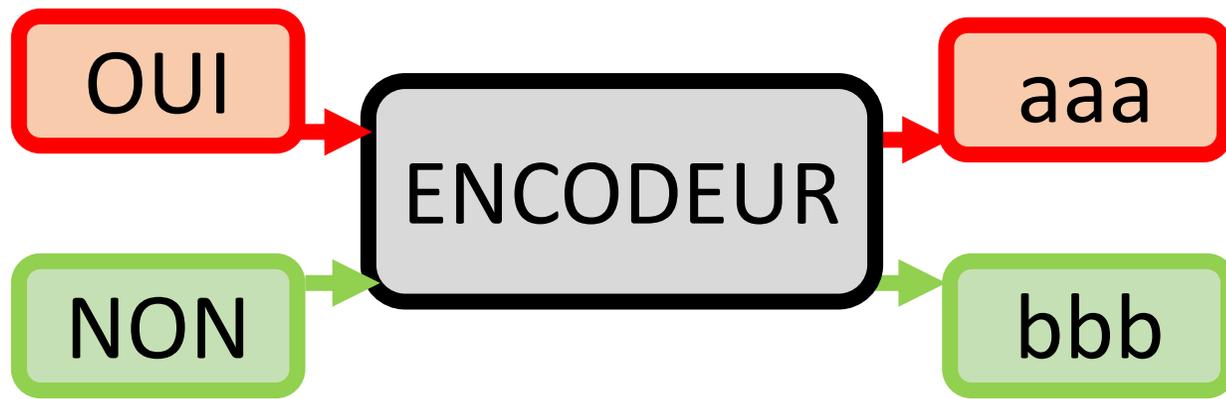
- **A** alphabet
- **n** longueur
- $C \subseteq A^n$  **code** (en blocs)
- $c \in C$  **mot** du code



# ENCODEUR

- $A = \{ a, b \}$
- $n = 3$
- $A^3 = \{ aaa, aab, aba, abb, baa, bab, bba, bbb \}$
- $C = \{ aaa, bbb \}$





- $C = \{ aaa, bbb \}$



# ENCODEUR

- pour  $c, c' \in C$ ,  
$$d(c, c') = \#\{ i \mid c_i \neq c'_i \}$$
  
(distance de Hamming)
- **Distance minimale.**



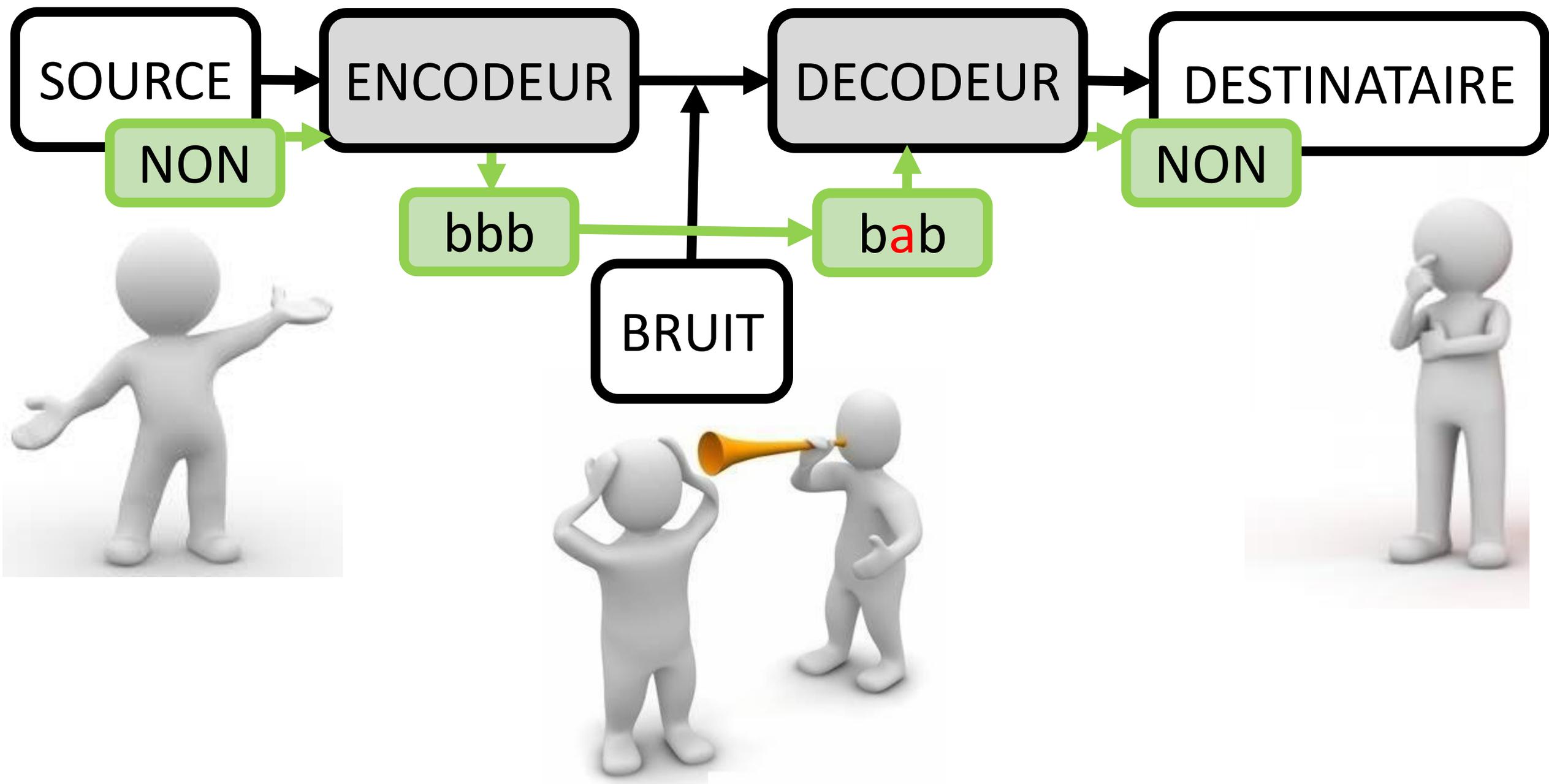
# ENCODEUR

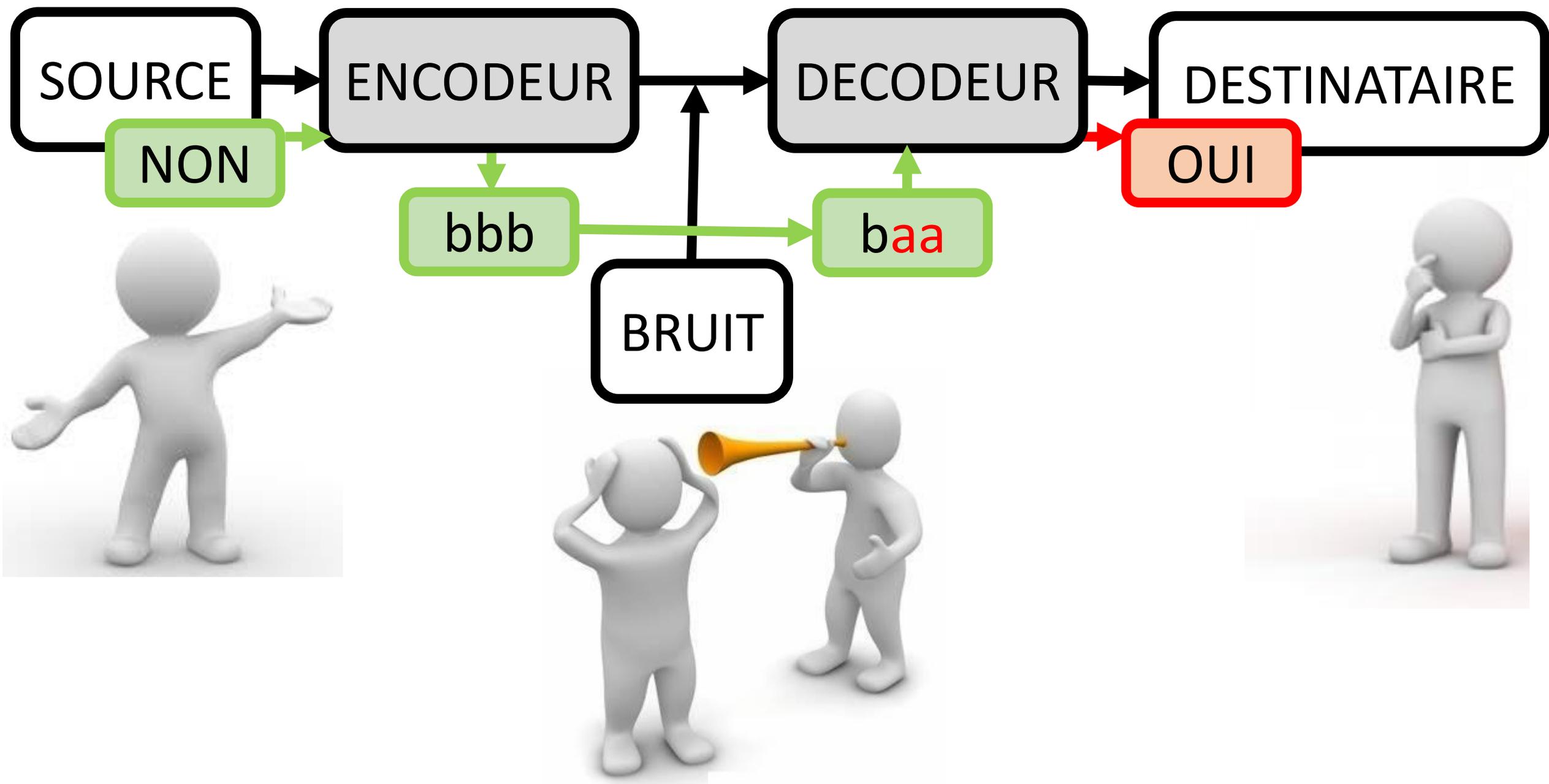
- pour  $c = aaa$  et  $c' = bbb$

$$d(c, c') = 3$$

- Distance minimale 3.

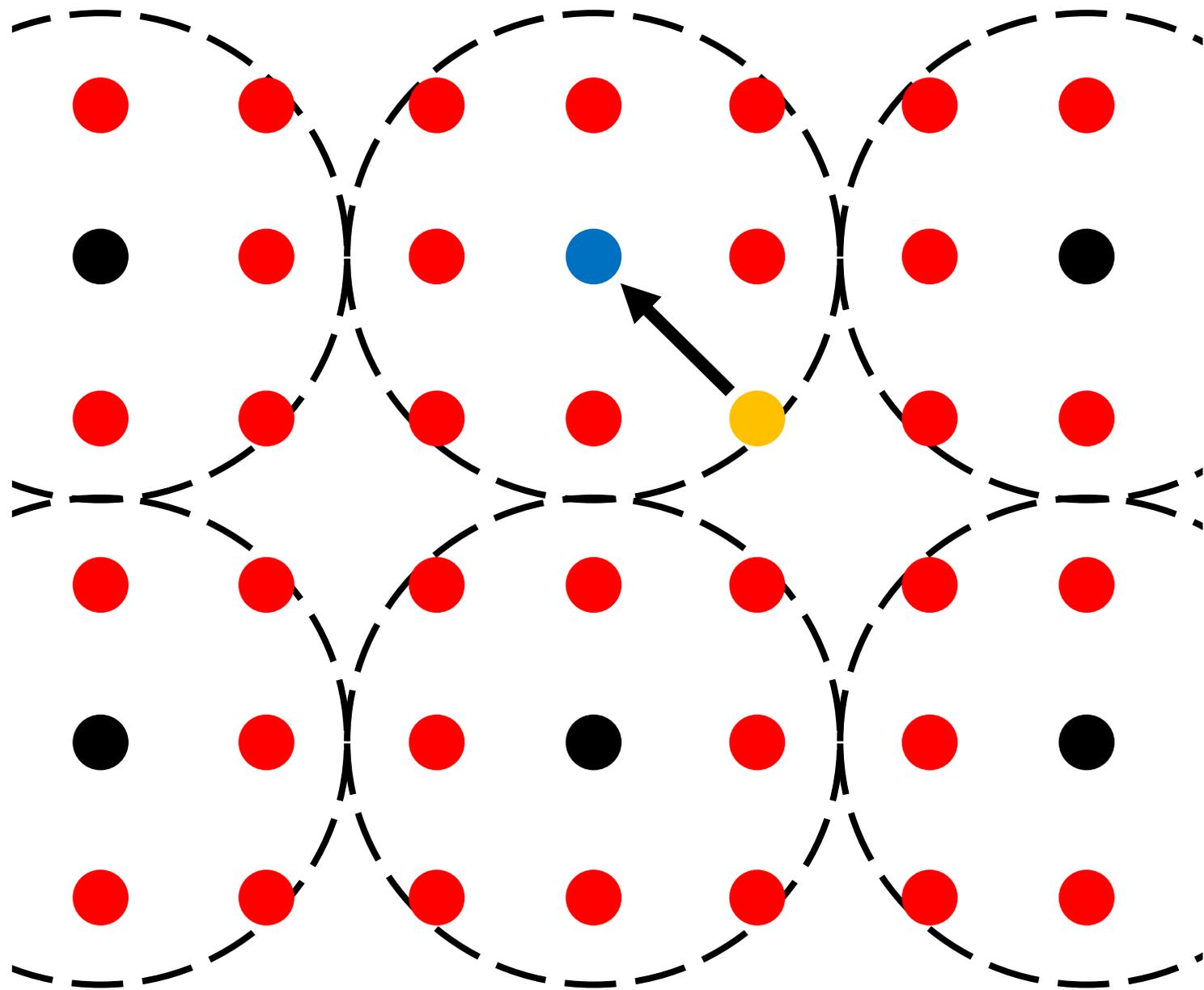








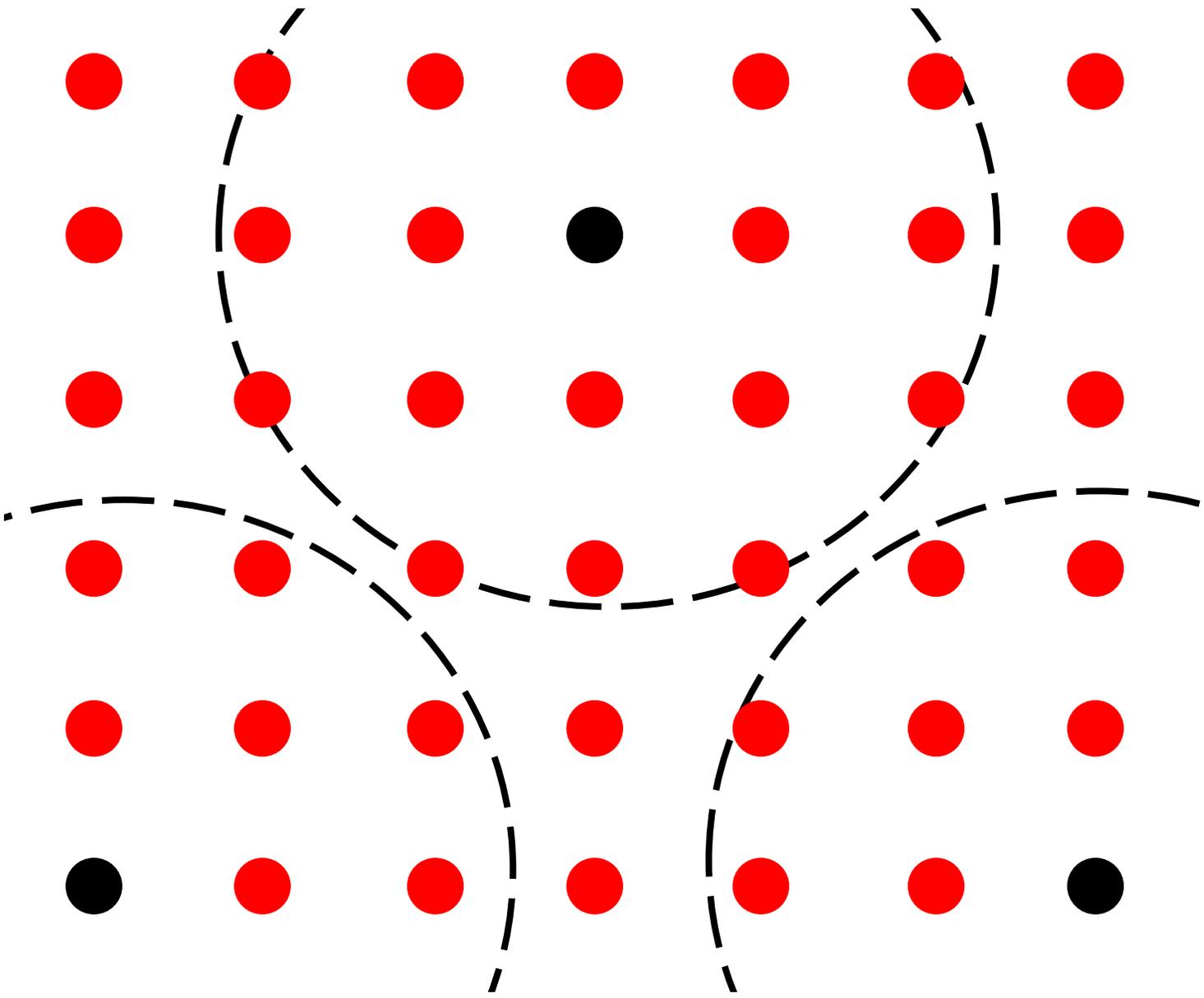




- = mots du code
- = mot émis
- = mot reçu

DECODEUR

● = mots du code





- $A = \{ a , b \}$
- $C \subseteq A^n$  capable de corriger 1 erreur

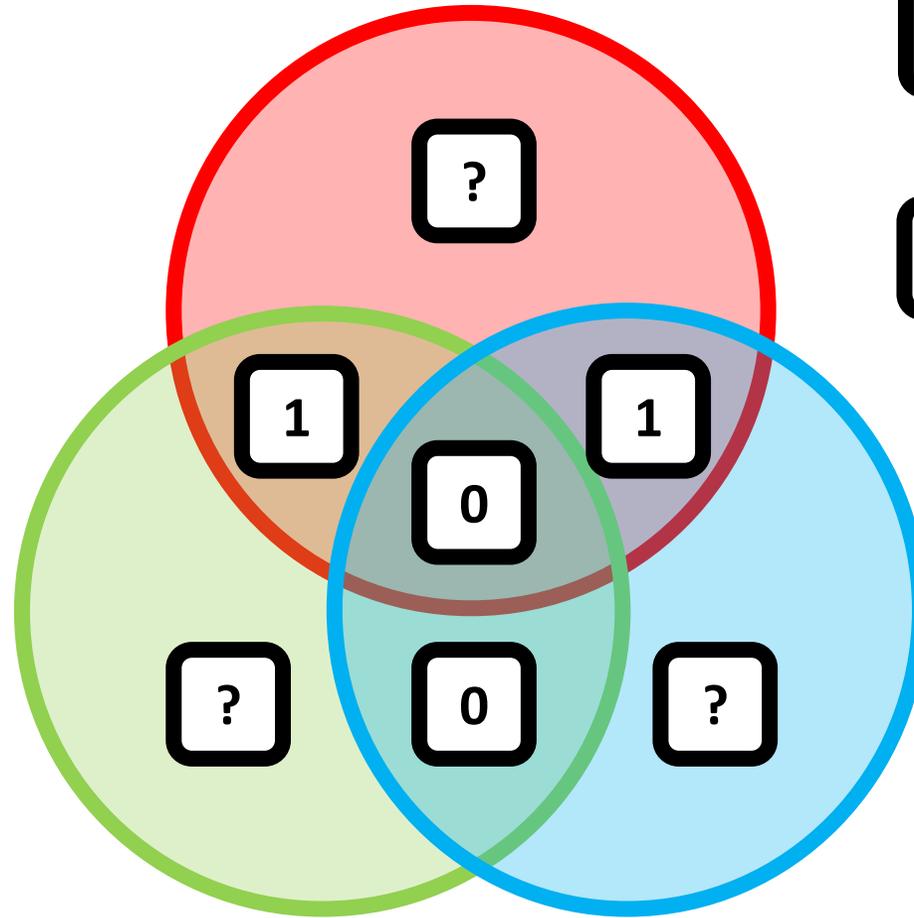
$$\#C \leq \frac{2^n}{n+1}$$



- $A = \{ a , b \}$
- $C \subseteq A^7$  capable de corriger 1 erreur

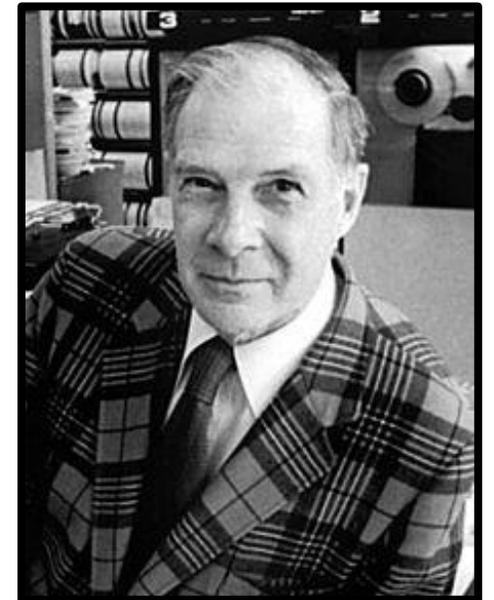
$$\#C \leq \frac{2^7}{7 + 1} = 16$$

- $A = \{ \boxed{0}, \boxed{1} \}$
- $n = 7$

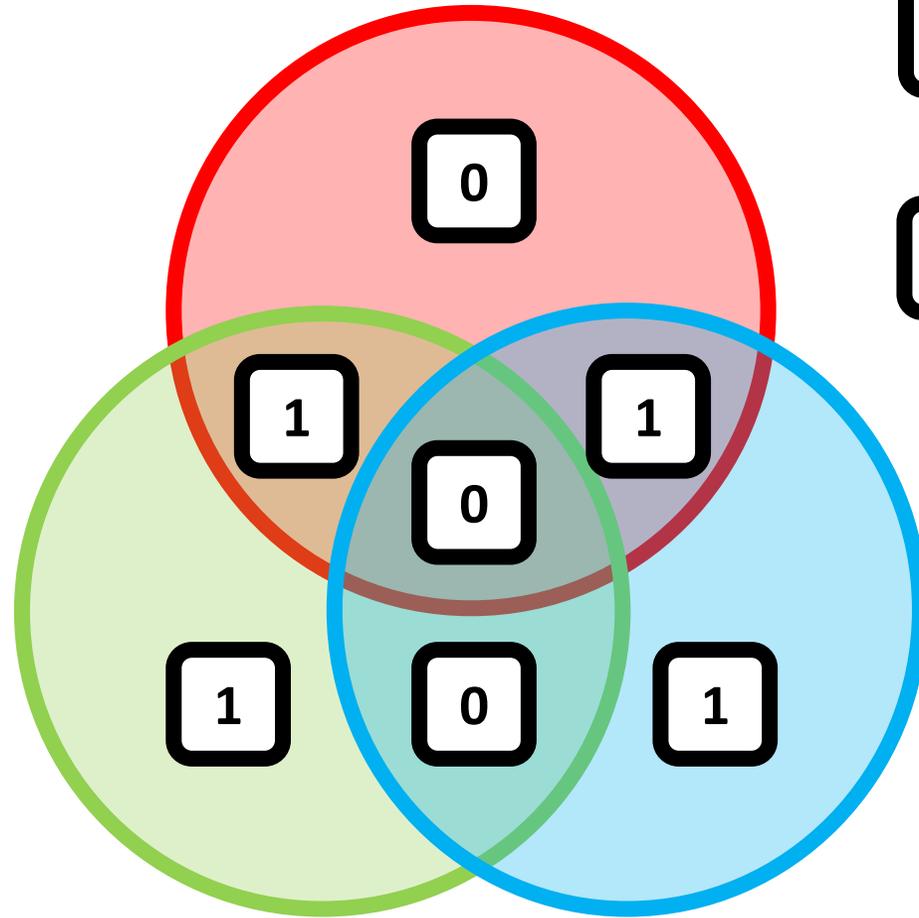


$\boxed{?} = \boxed{0}$  si nombre pair  
de 1 dans le cercle

$\boxed{?} = \boxed{1}$  autrement

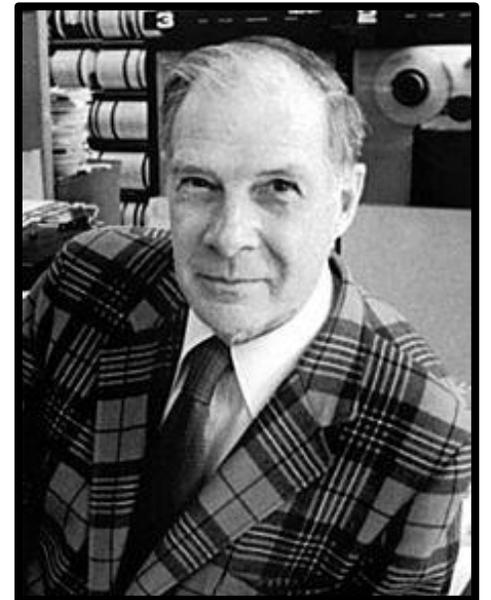


- $A = \{ \boxed{0}, \boxed{1} \}$
- $n = 7$

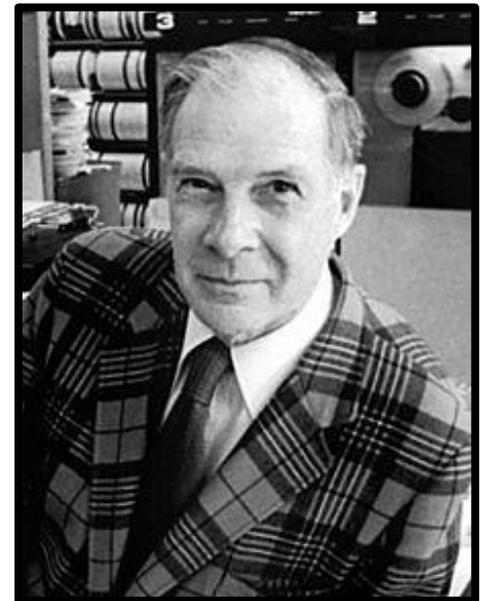
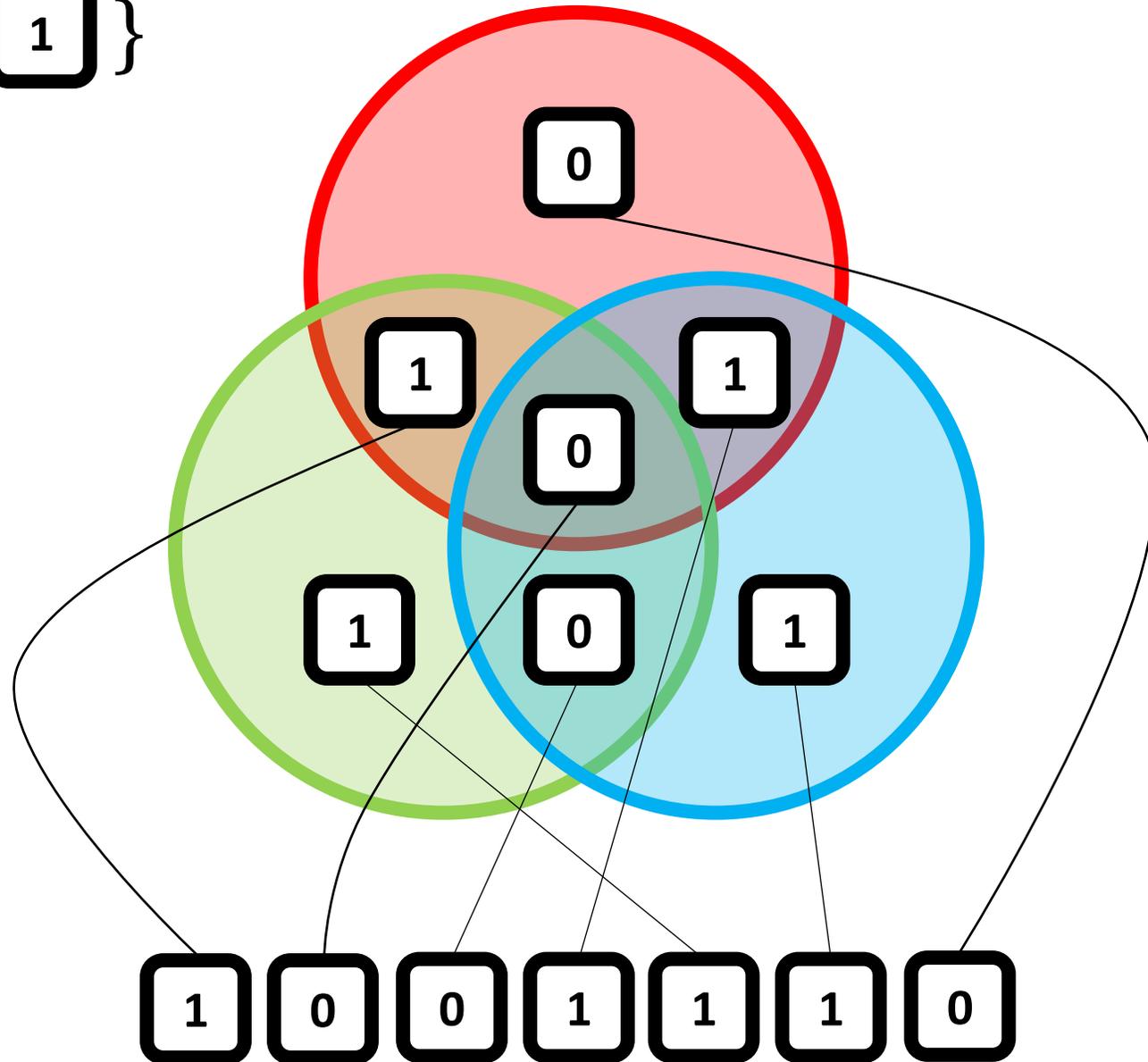


$\boxed{?} = \boxed{0}$  si nombre pair  
de 1 dans le cercle

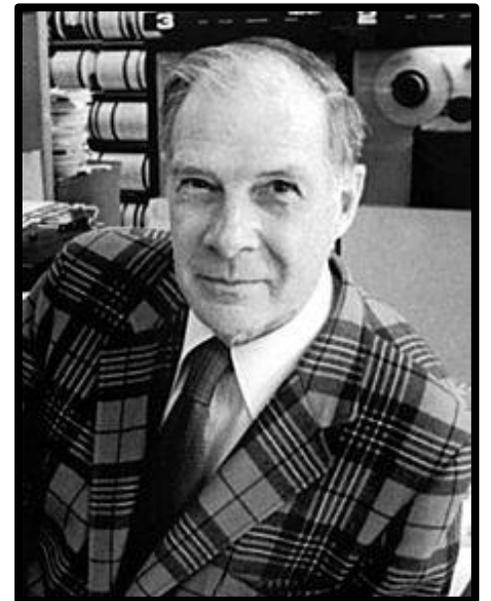
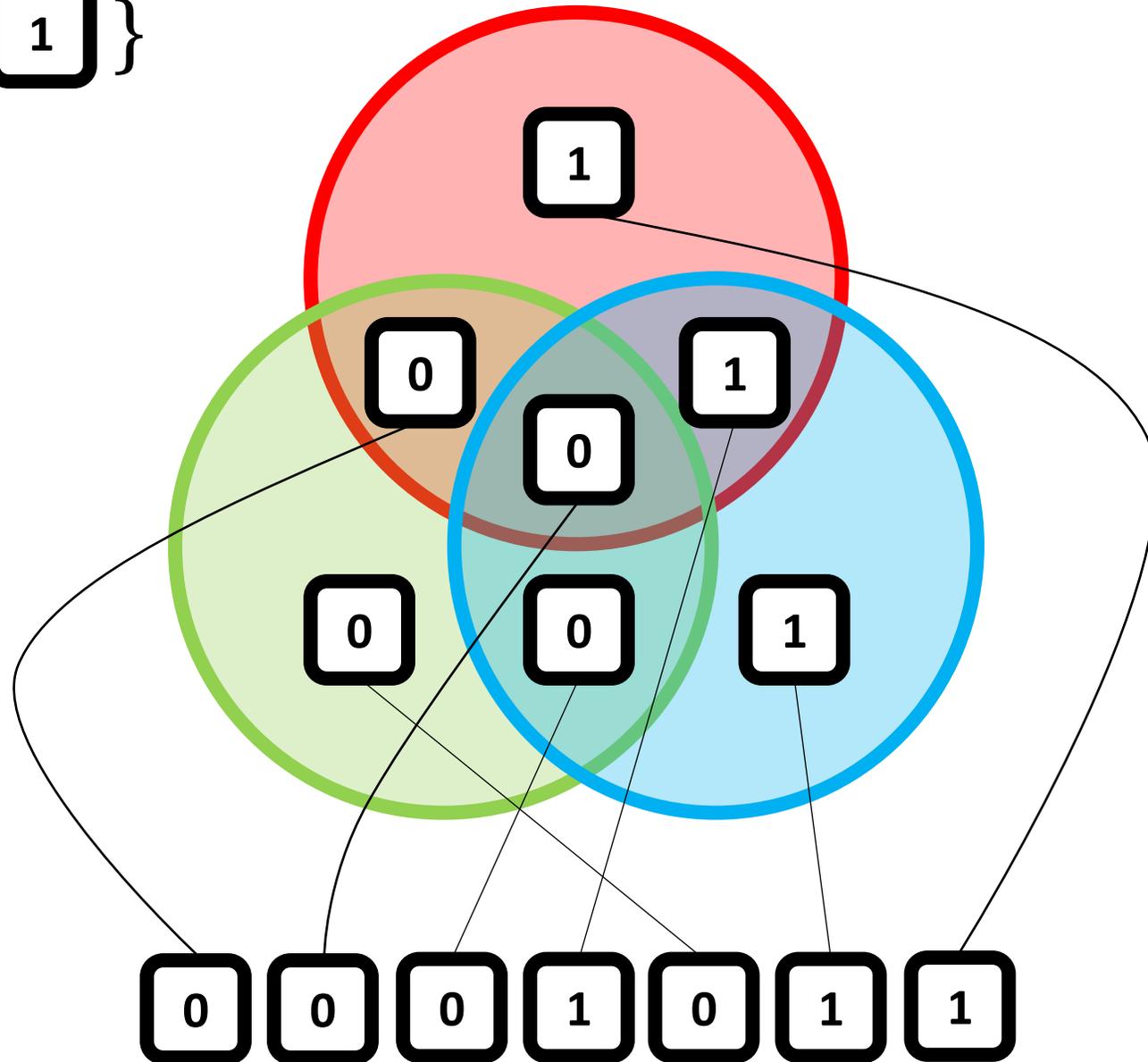
$\boxed{?} = \boxed{1}$  autrement



- $A = \{ \boxed{0}, \boxed{1} \}$
- $n = 7$



- $A = \{ \boxed{0}, \boxed{1} \}$
- $n = 7$

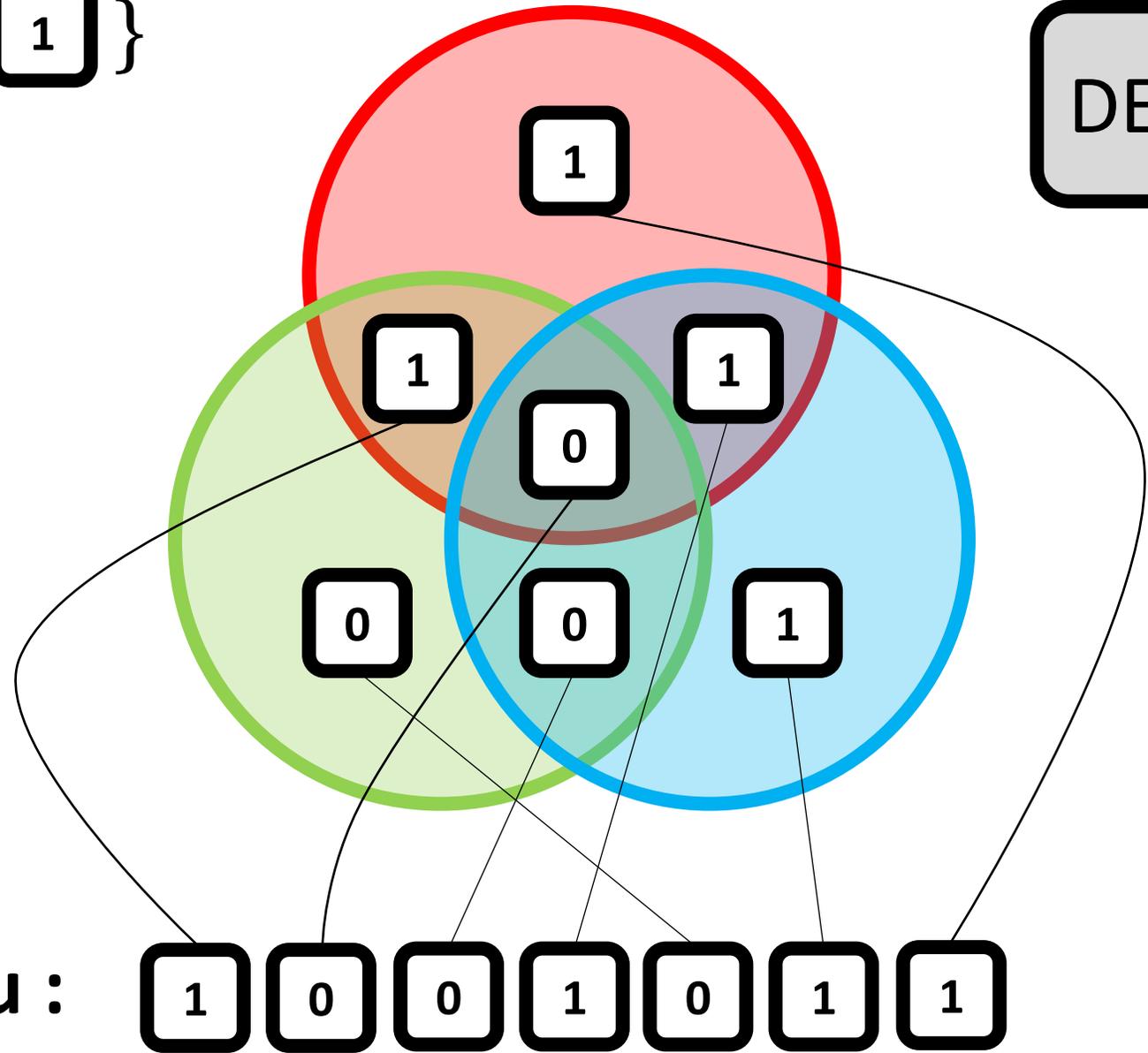


0	0	0	0	0	0	0
0	0	0	1	0	1	1
0	0	1	0	1	1	0
0	0	1	1	1	0	1
0	1	0	0	1	1	1
0	1	0	1	1	0	0
0	1	1	0	0	0	1
0	1	1	1	0	1	0

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

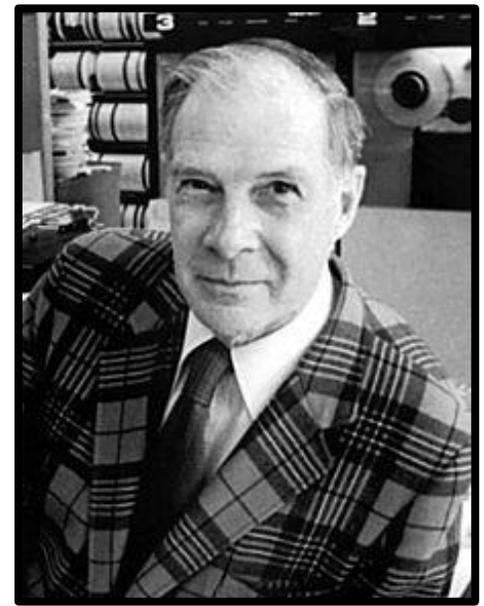
- $A = \{ \boxed{0}, \boxed{1} \}$
- $n = 7$
- $\# C = 16$

DECODEUR



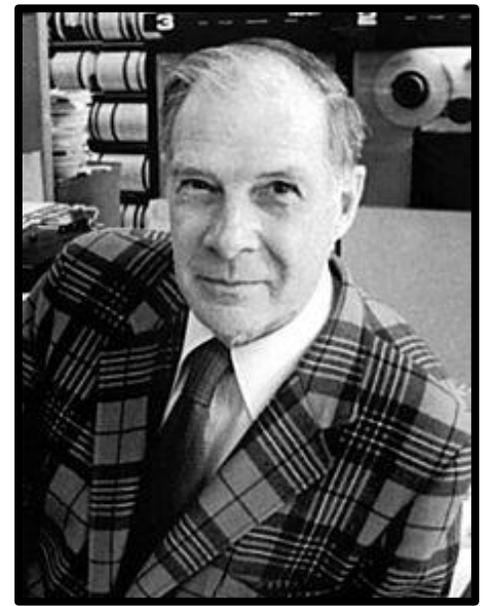
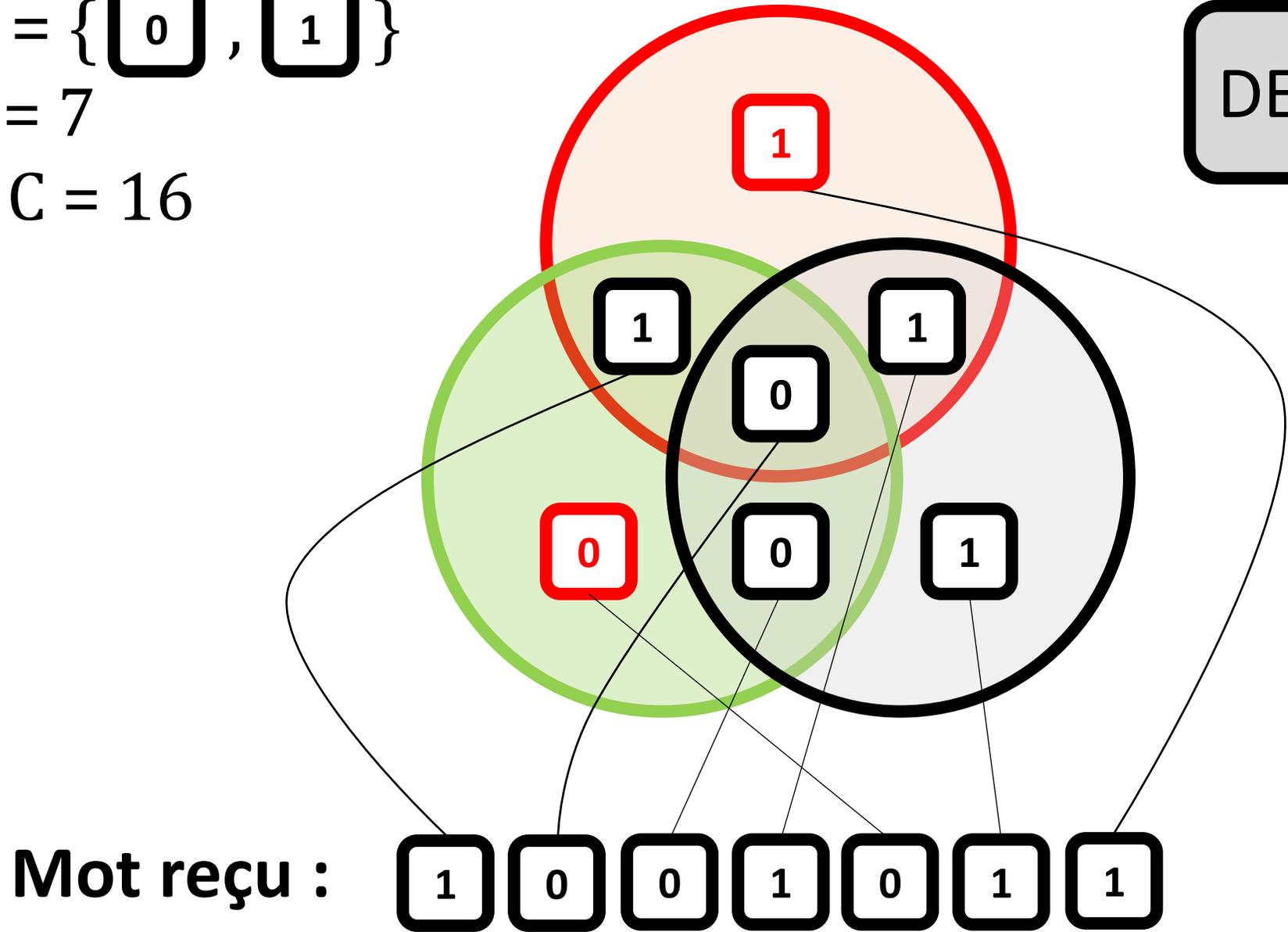
Mot reçu :

**1 0 0 1 0 1 1**



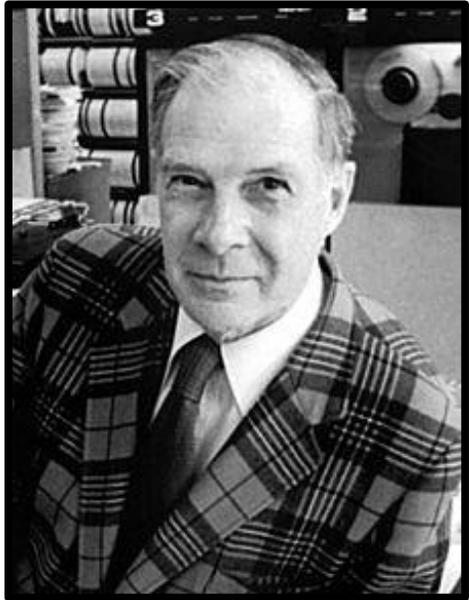
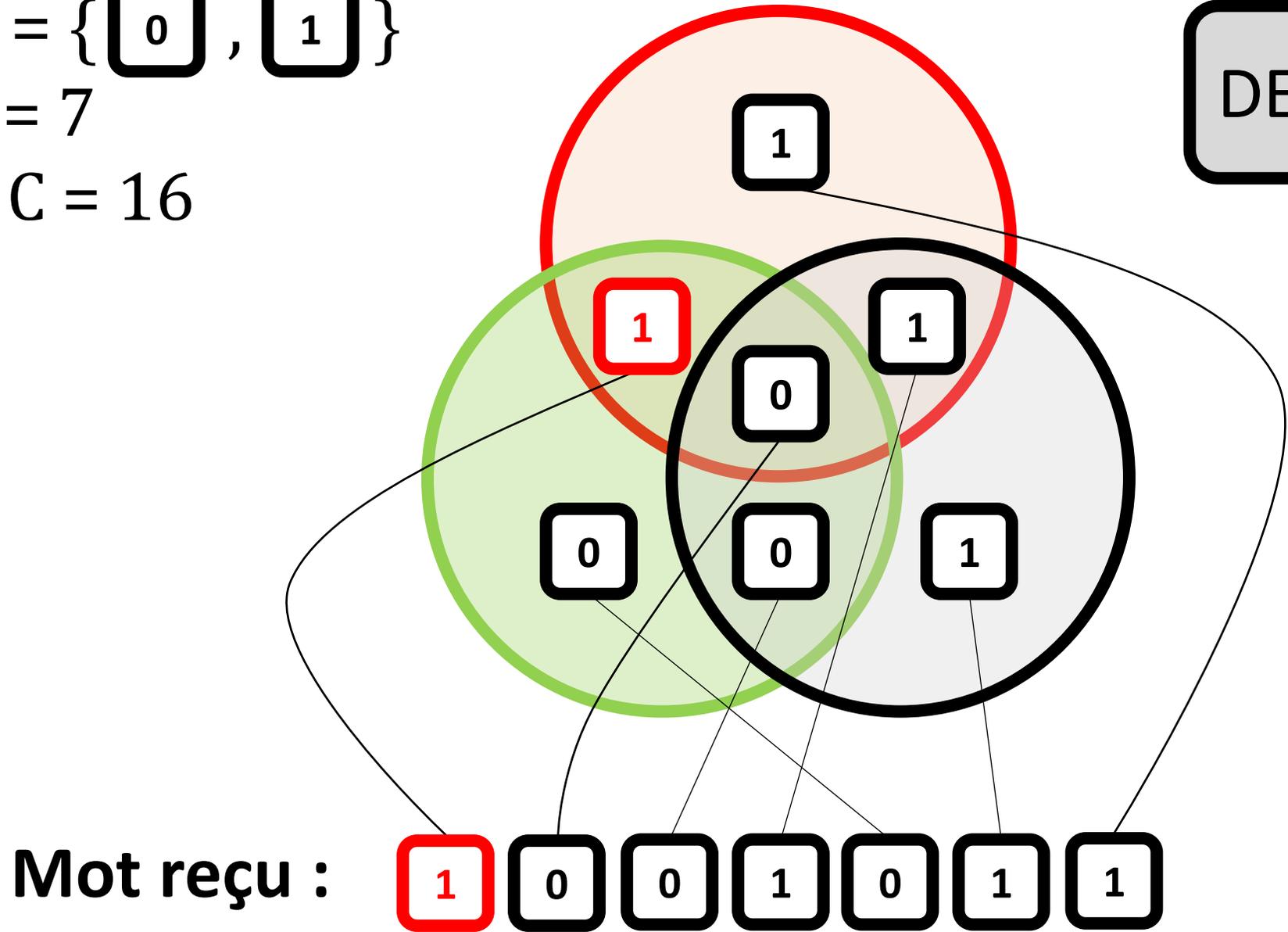
- $A = \{ \boxed{0}, \boxed{1} \}$
- $n = 7$
- $\# C = 16$

DECODEUR



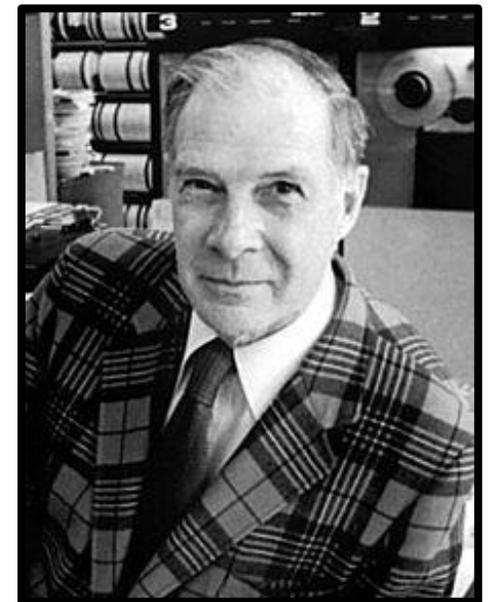
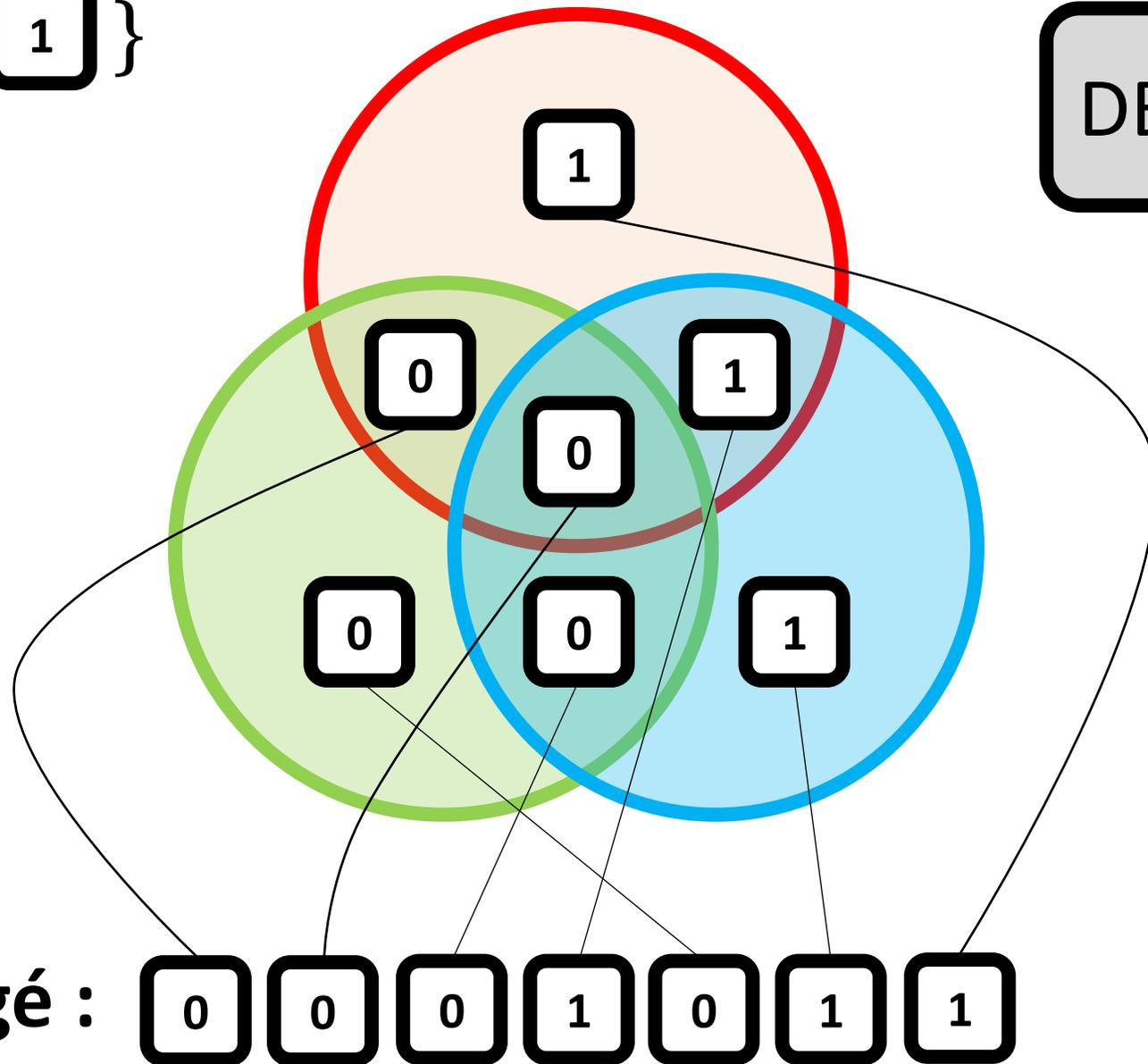
- $A = \{ \boxed{0}, \boxed{1} \}$
- $n = 7$
- $\# C = 16$

DECODEUR



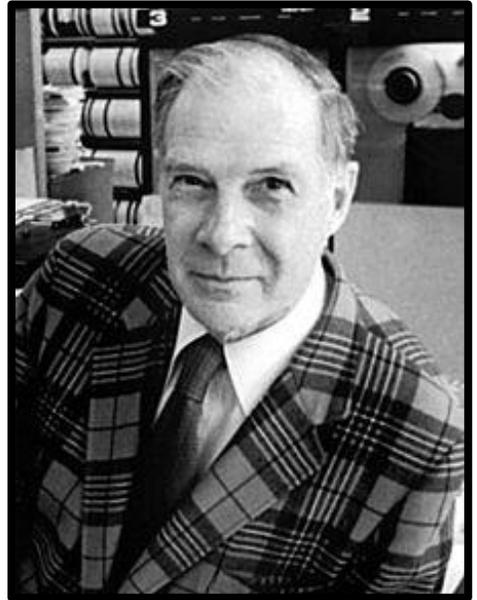
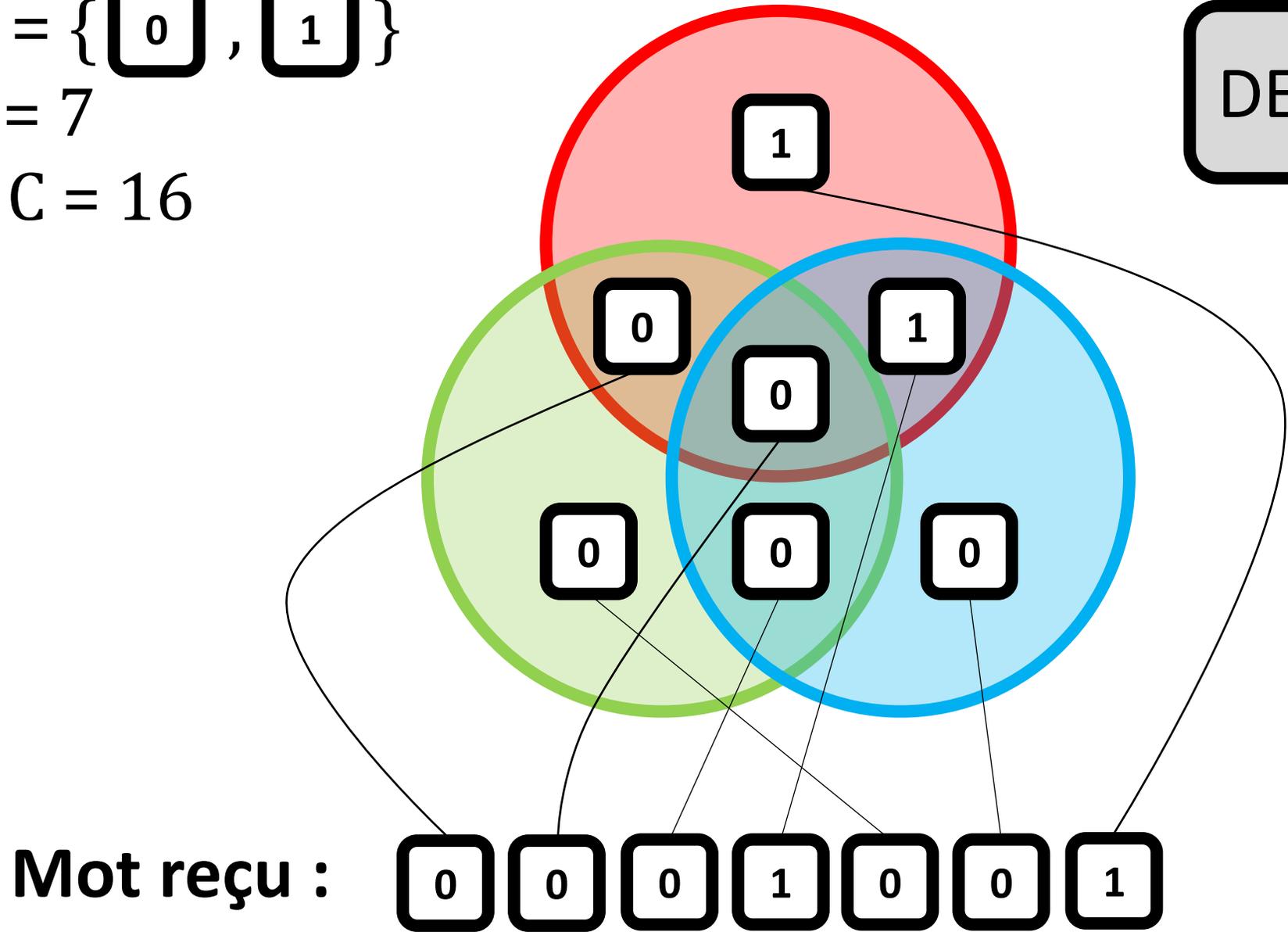
- $A = \{ \boxed{0}, \boxed{1} \}$
- $n = 7$
- $\# C = 16$

DECODEUR



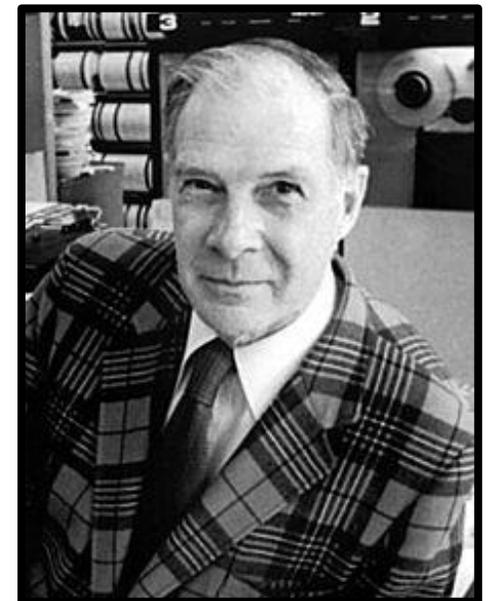
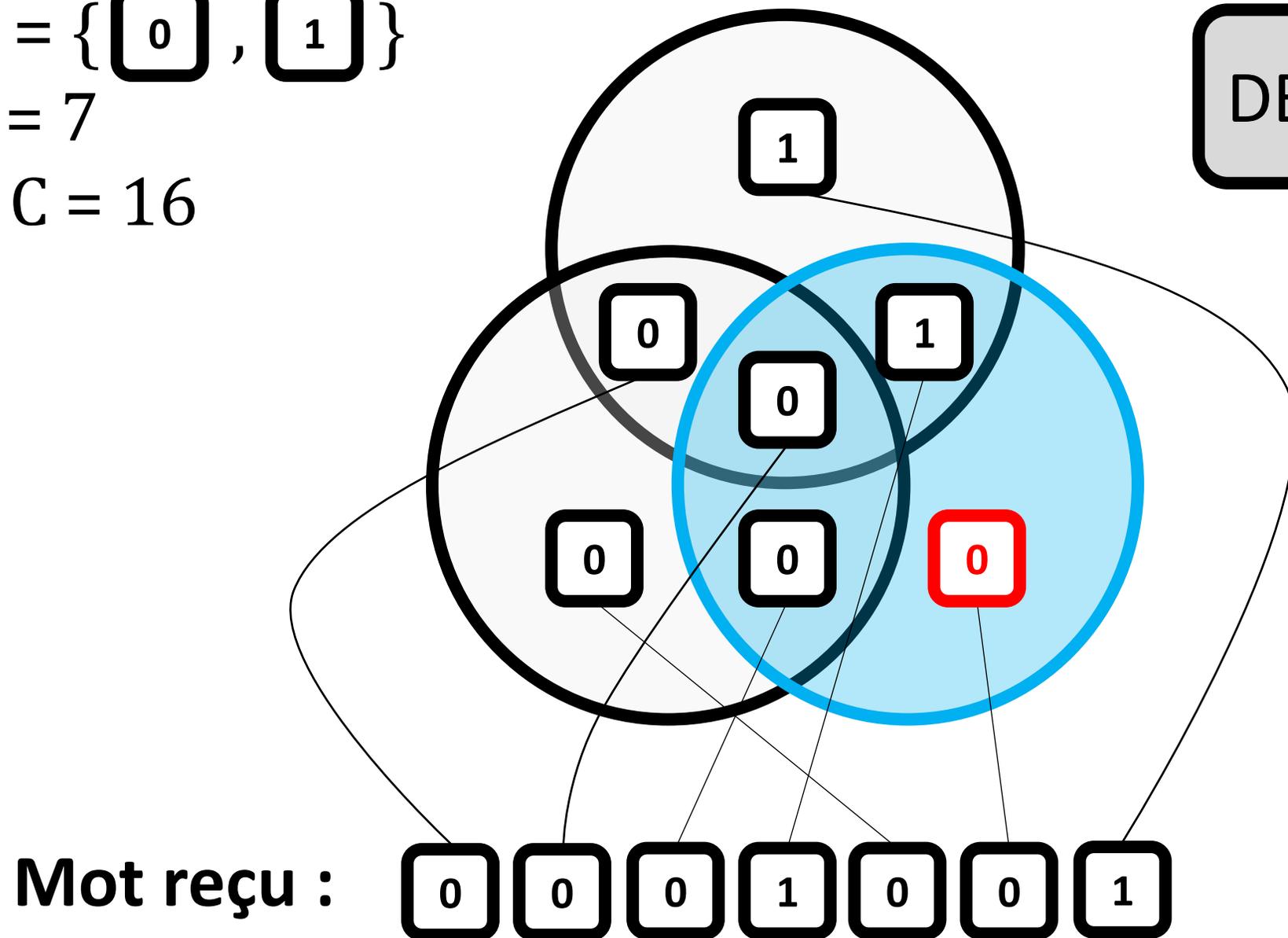
- $A = \{ \boxed{0}, \boxed{1} \}$
- $n = 7$
- $\# C = 16$

DECODEUR



- $A = \{ \boxed{0}, \boxed{1} \}$
- $n = 7$
- $\# C = 16$

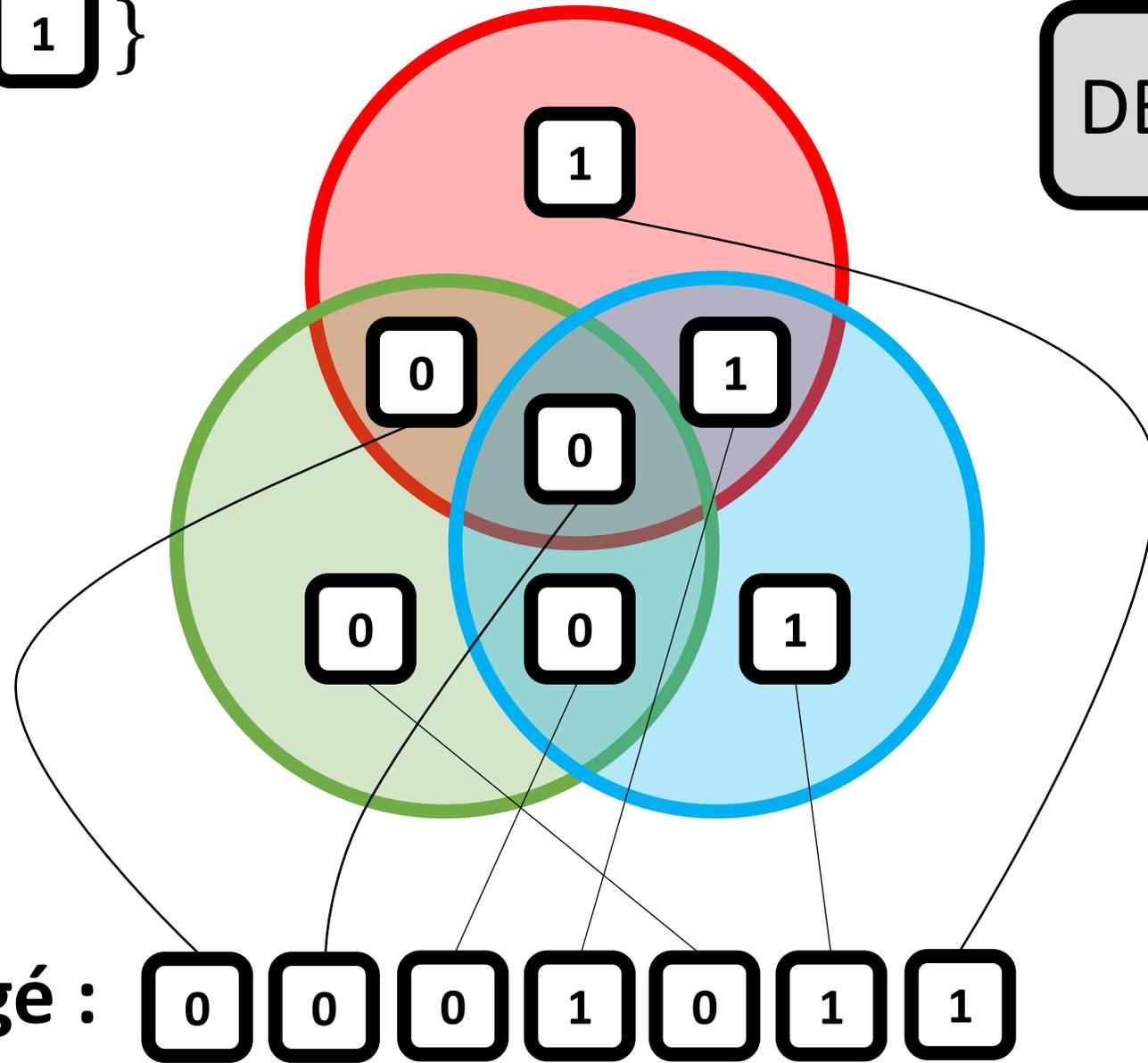
DECODEUR



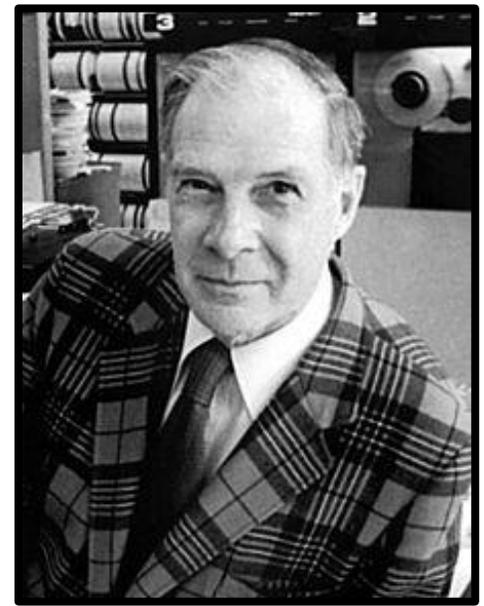


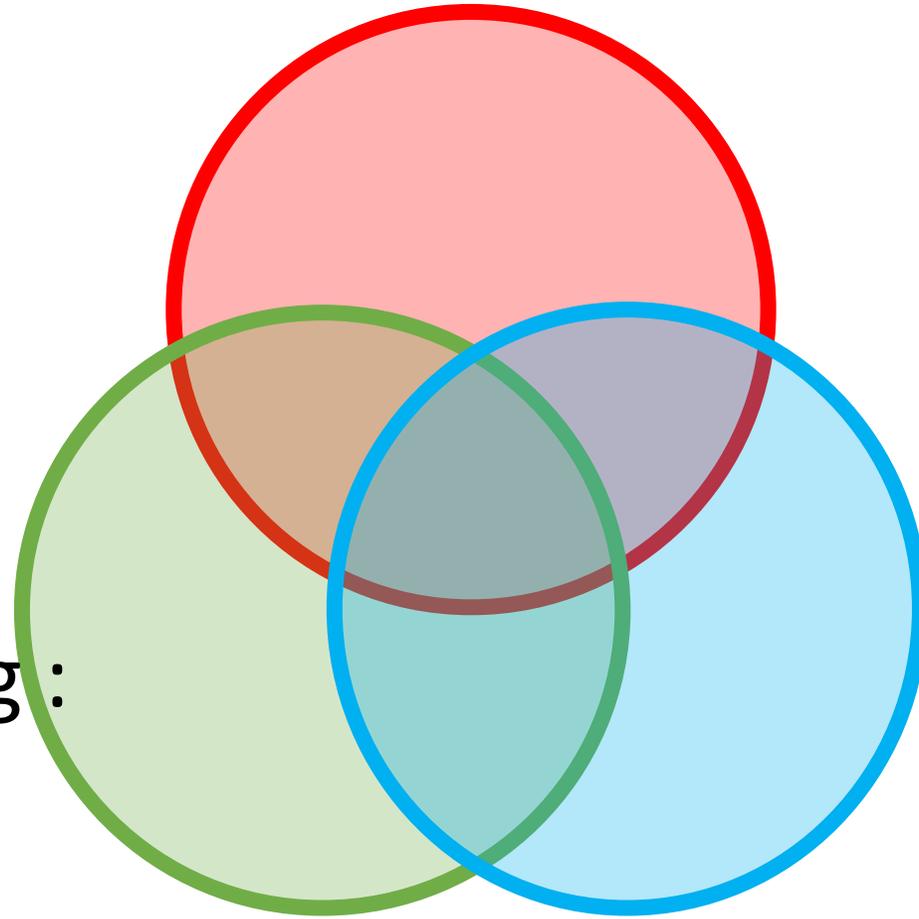
- $A = \{ \boxed{0}, \boxed{1} \}$
- $n = 7$
- $\# C = 16$

DECODEUR



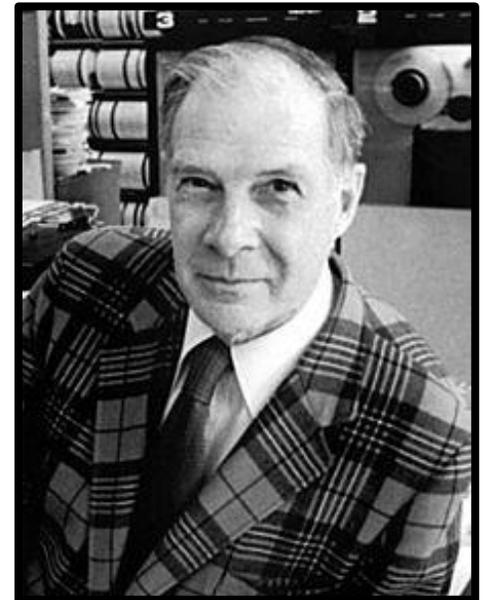
Mot corrigé : **0 0 0 1 0 1 1**

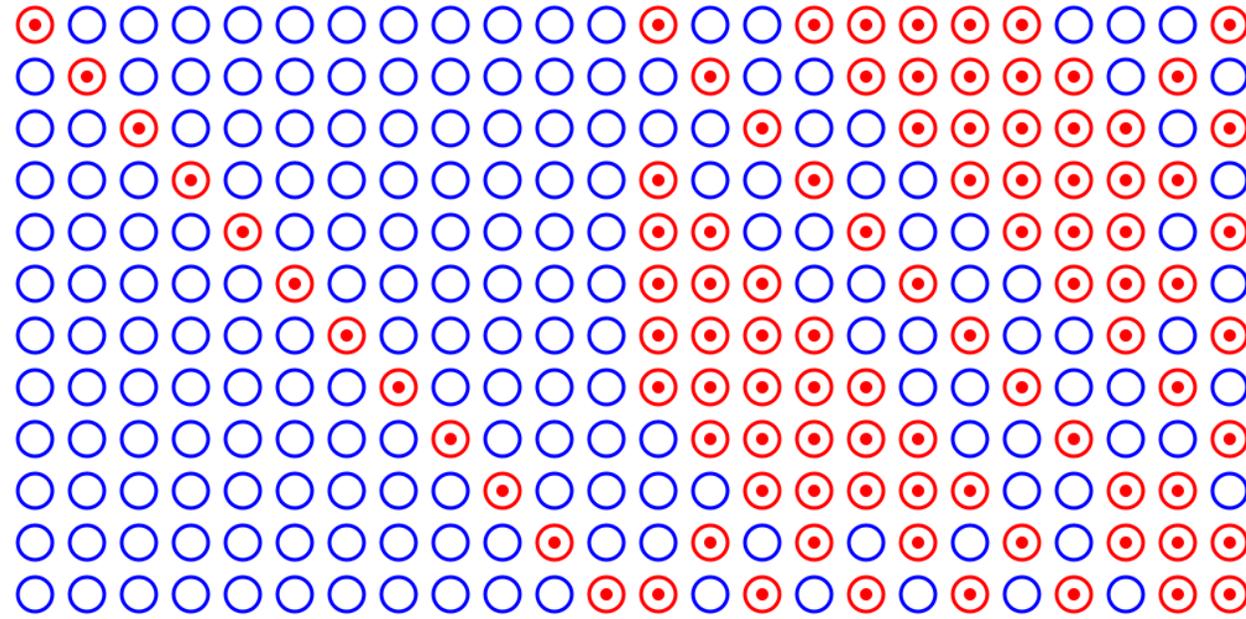
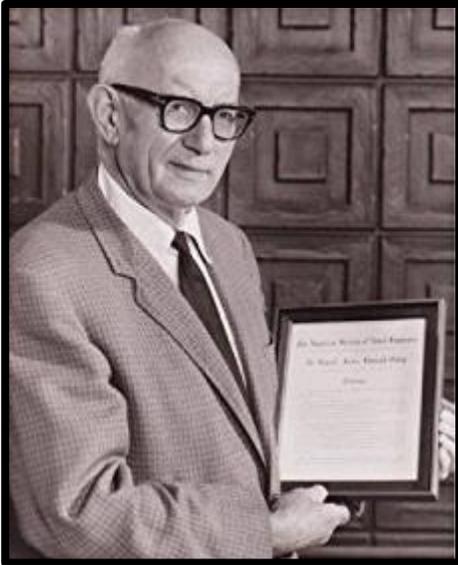




Code de Hamming :

- longueur 7;
- 16 mots;
- capable de corriger 1 erreurs.





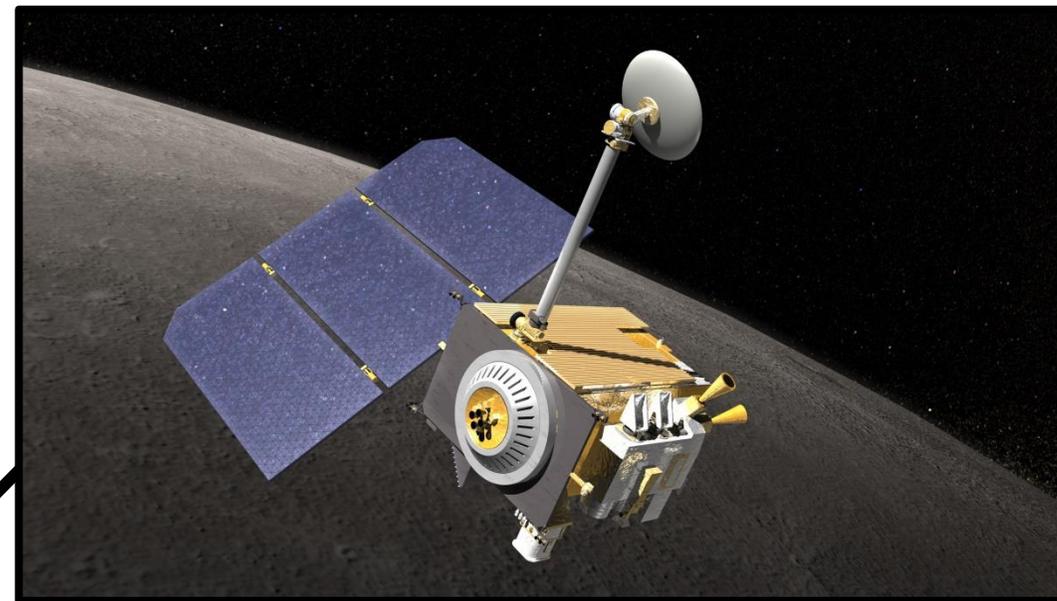
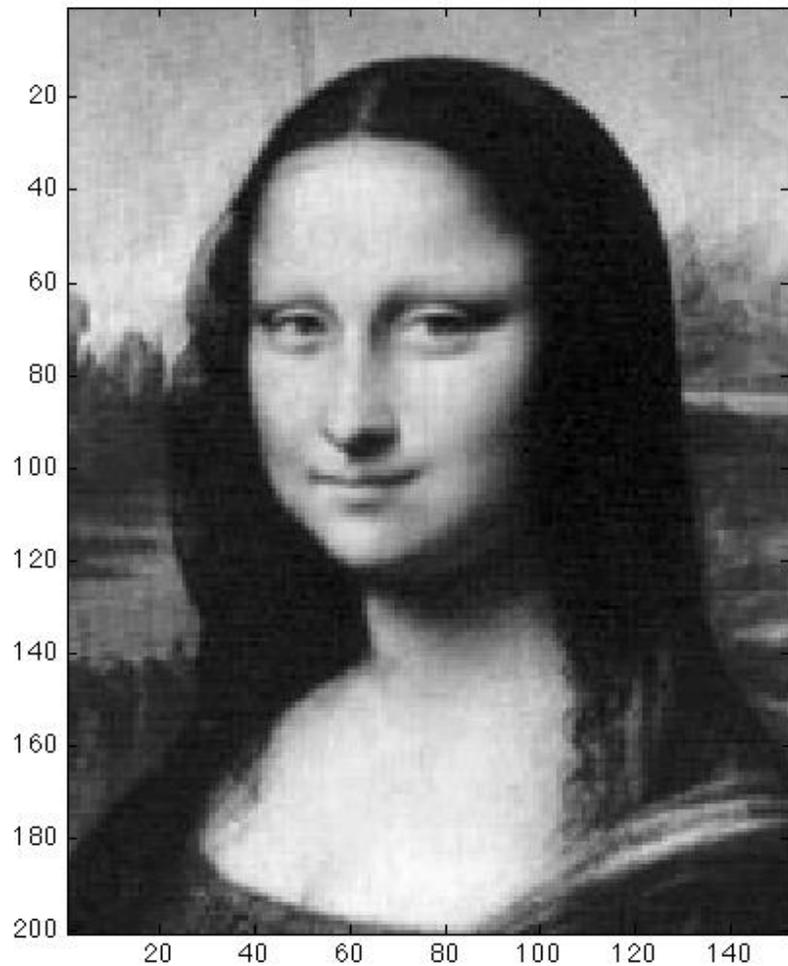
Code de Golay :

- longueur 24;
- 4096 mots;
- capable de corriger 3 erreurs.



Sonde spatiale **Voyager 1**

# Image transmise de la terre

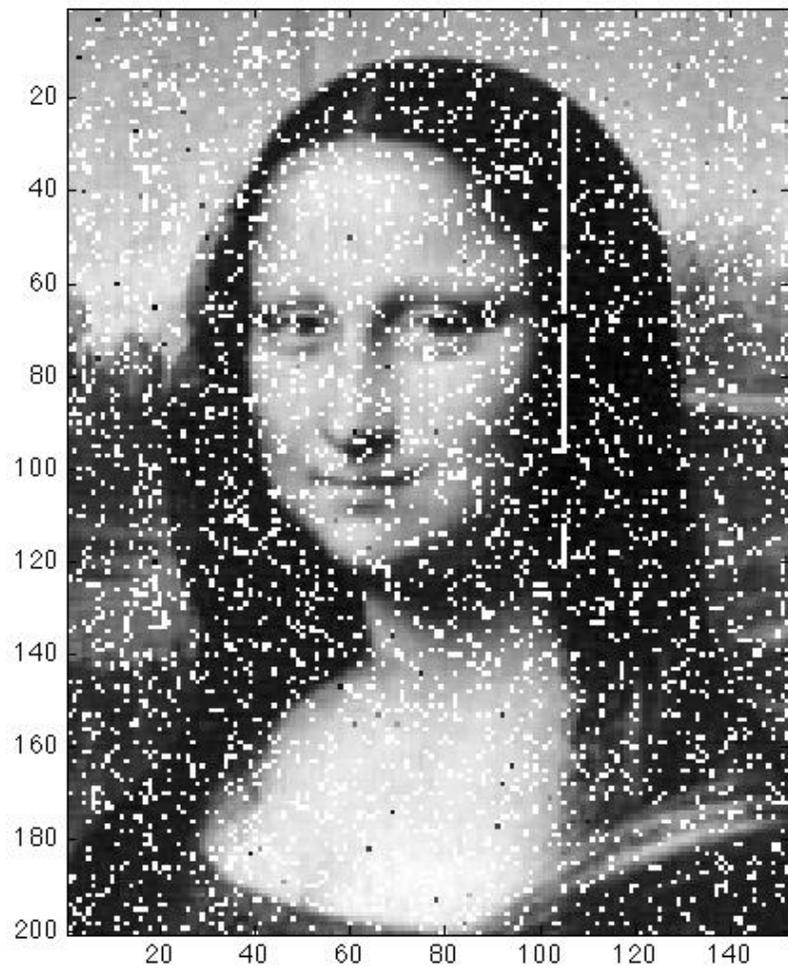


NASA's Lunar Reconnaissance Orbiter (LRO)

**BRUIT**



Image reçue (sans code)



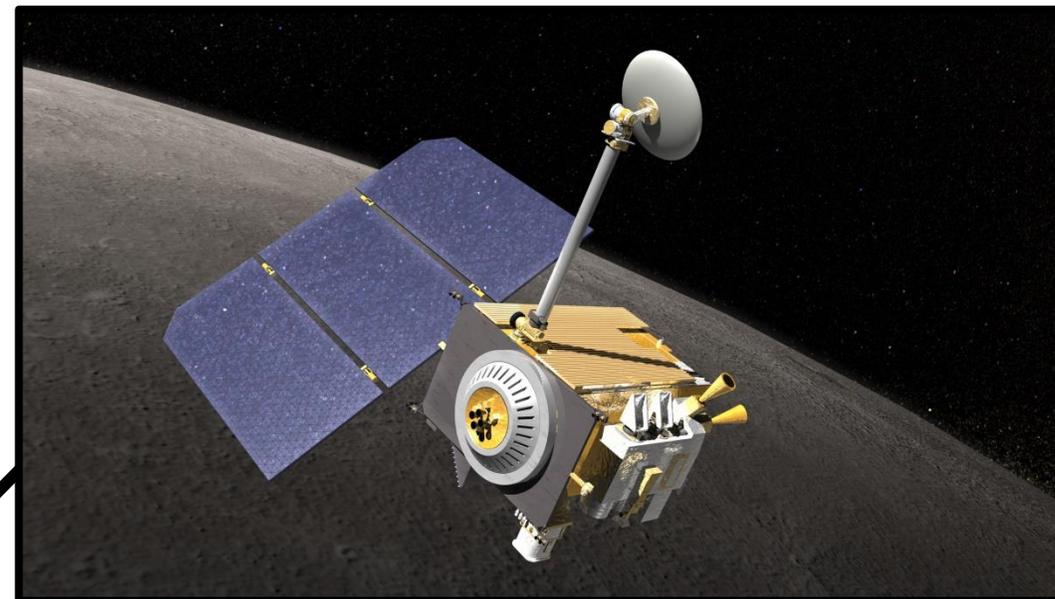
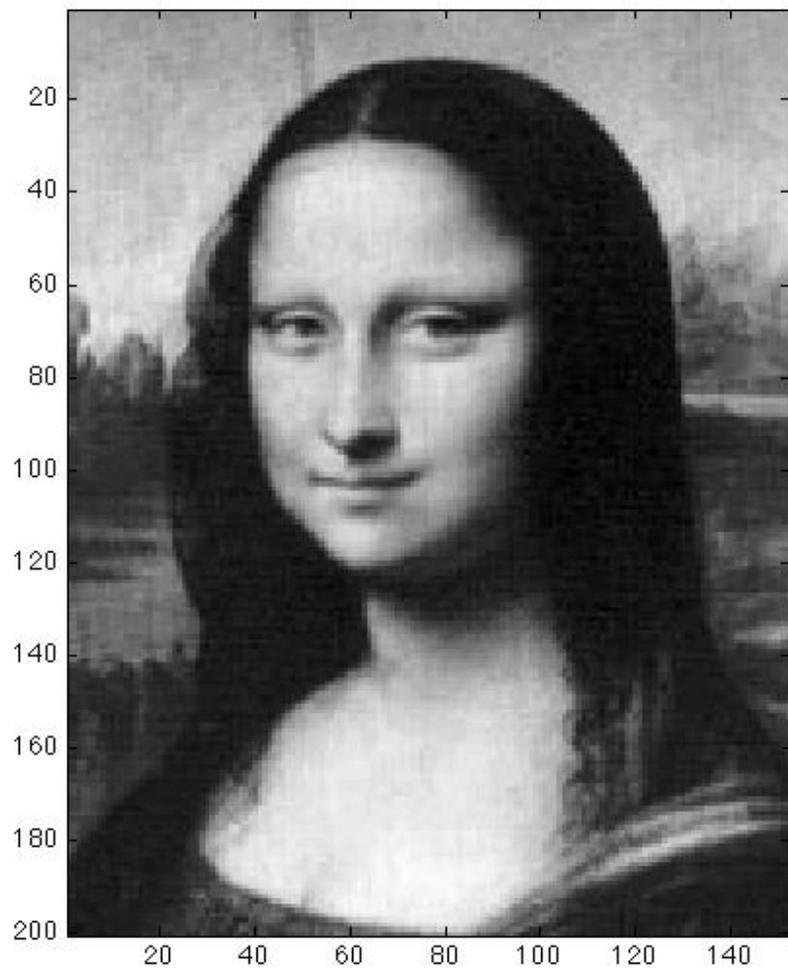
BRUIT



NASA's Lunar Reconnaissance Orbiter (LRO)



## Image reçue avec code (de Reed-Solomon)



NASA's Lunar Reconnaissance Orbiter (LRO)

BRUIT



Irving S. Reed et Gustave Solomon

MERCI POUR  
L'ATTEN**N**ION !

