

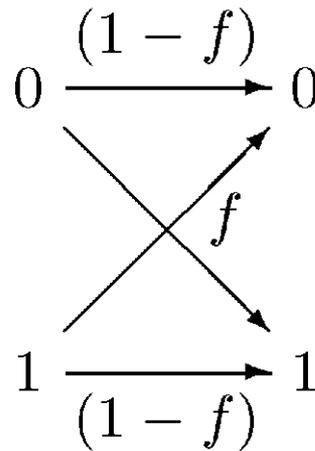
# Transmission fiable et codes correcteurs

---

Marc Lelarge (INRIA-ENS)

Olympiades de mathématiques - Sorbonne 2010.

# Canal Binaire Symétrique (CBS)



# Code à répétition R3

Bit d'information	<b>s</b>	0	0	1	0	1	1	0
Mot code transmis	<b>t</b>	$\overbrace{000}$	$\overbrace{000}$	$\overbrace{111}$	$\overbrace{000}$	$\overbrace{111}$	$\overbrace{111}$	$\overbrace{000}$
Bruit	<b>n</b>	000	001	000	000	101	000	000
Message reçu	<b>r</b>	000	001	111	000	010	111	000

# Décodage de R3

<b>s</b>	0	0	1	0	1	1	0
<b>t</b>	$\underbrace{000}$	$\underbrace{000}$	$\underbrace{111}$	$\underbrace{000}$	$\underbrace{111}$	$\underbrace{111}$	$\underbrace{000}$
<b>n</b>	000	001	000	000	101	000	000
<b>r</b>	$\underbrace{000}$	$\underbrace{001}$	$\underbrace{111}$	$\underbrace{000}$	$\underbrace{010}$	$\underbrace{111}$	$\underbrace{000}$
<b><math>\hat{s}</math></b>	0	0	1	0	0	1	0

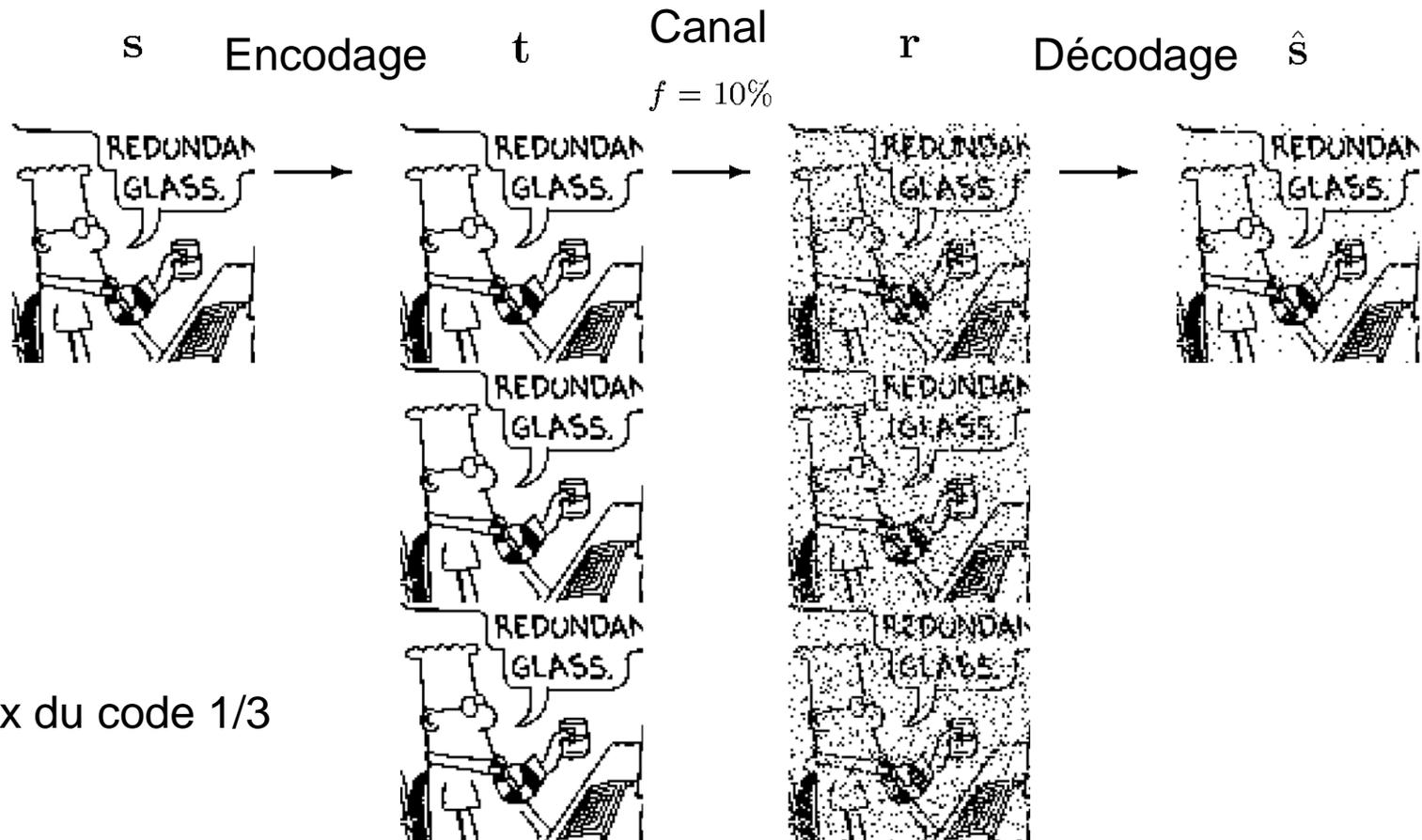
Erreurs corrigées

★

Erreurs détectées

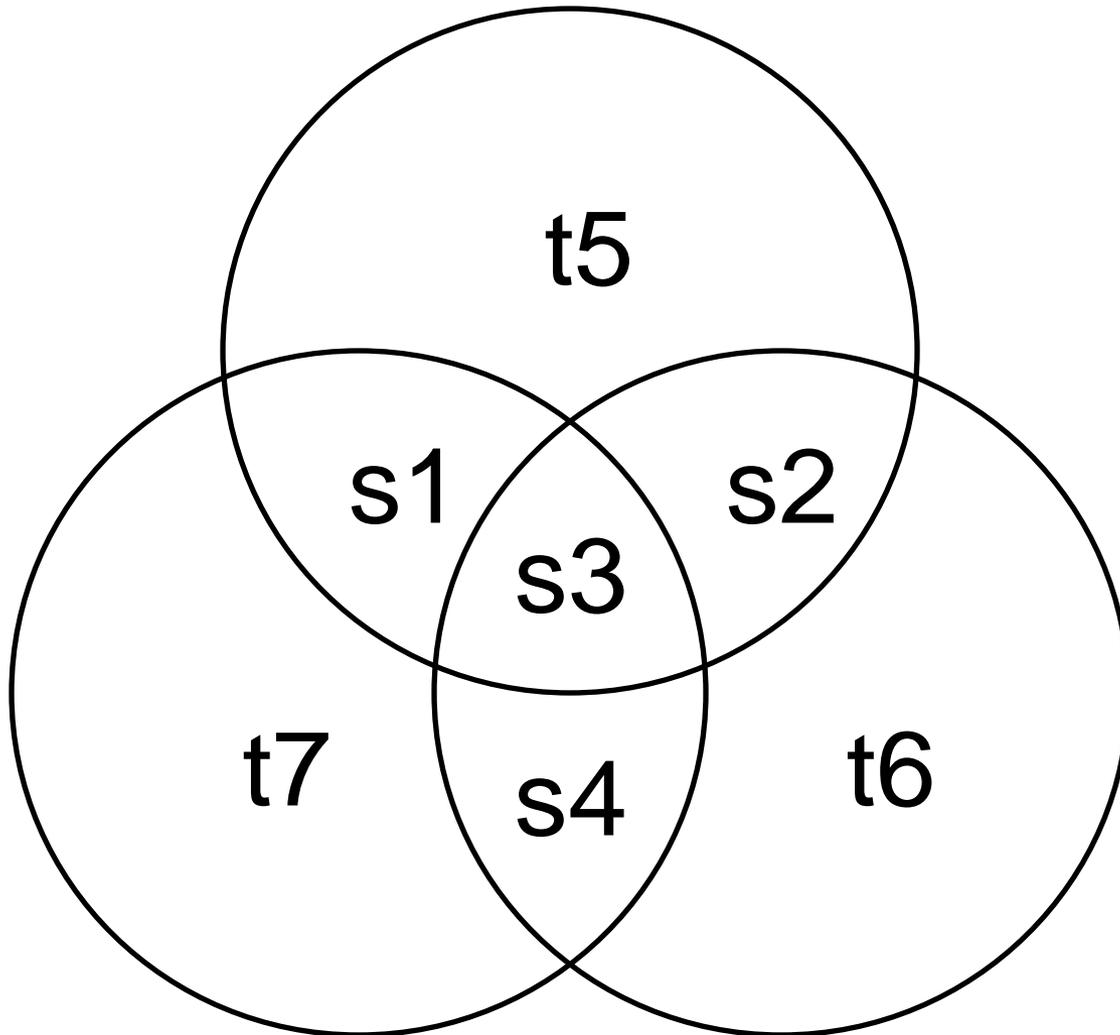
★

# Code à répétition

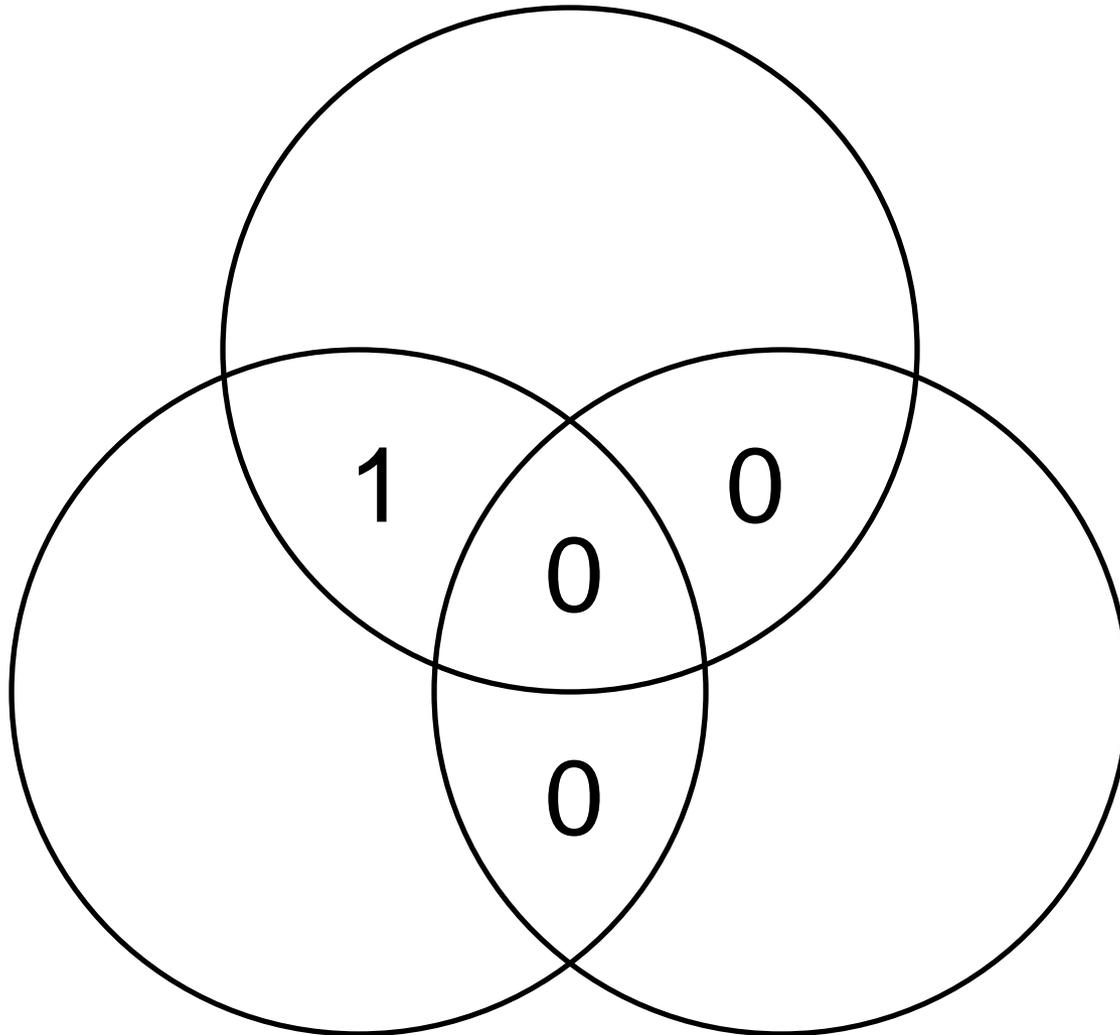


Taux du code 1/3

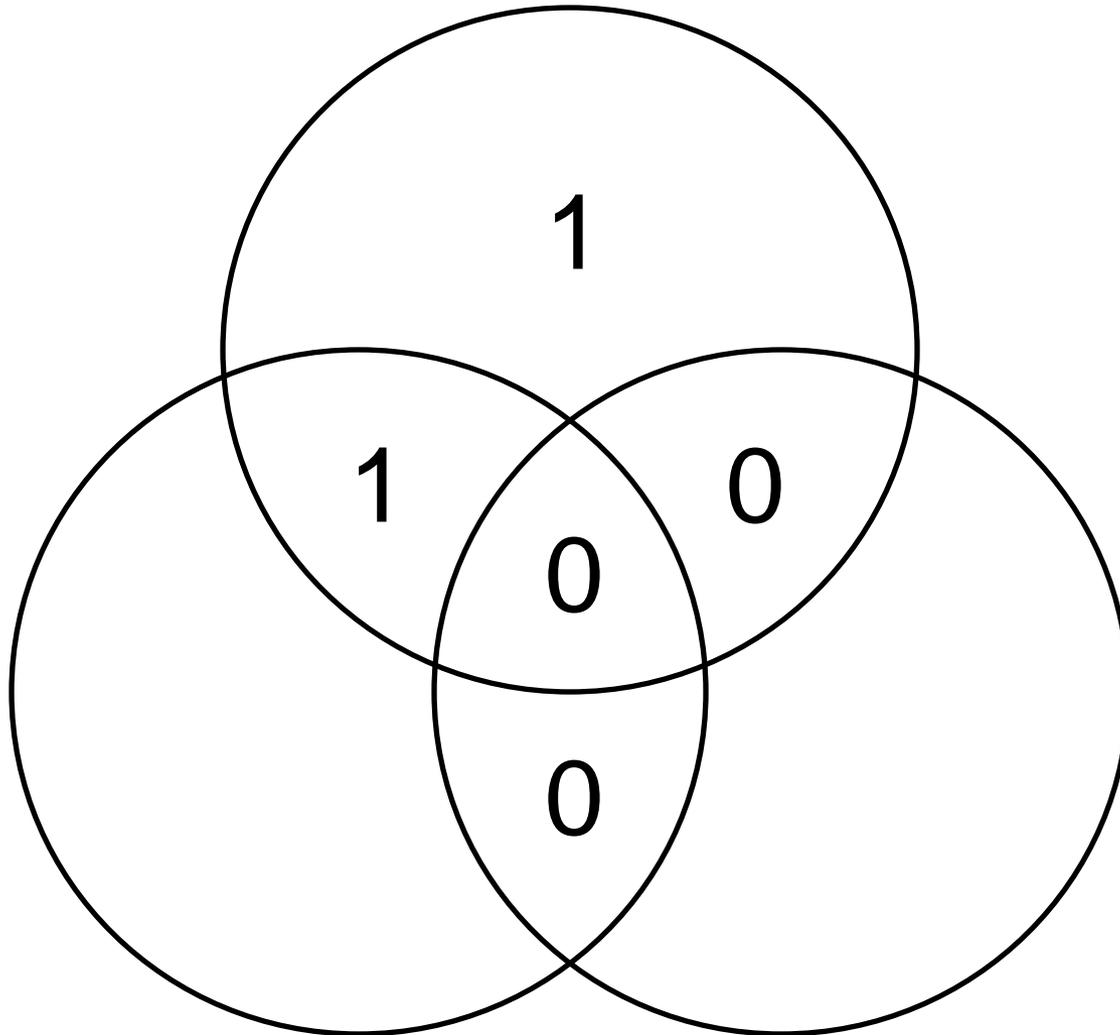
# Code de Hamming (7,4)



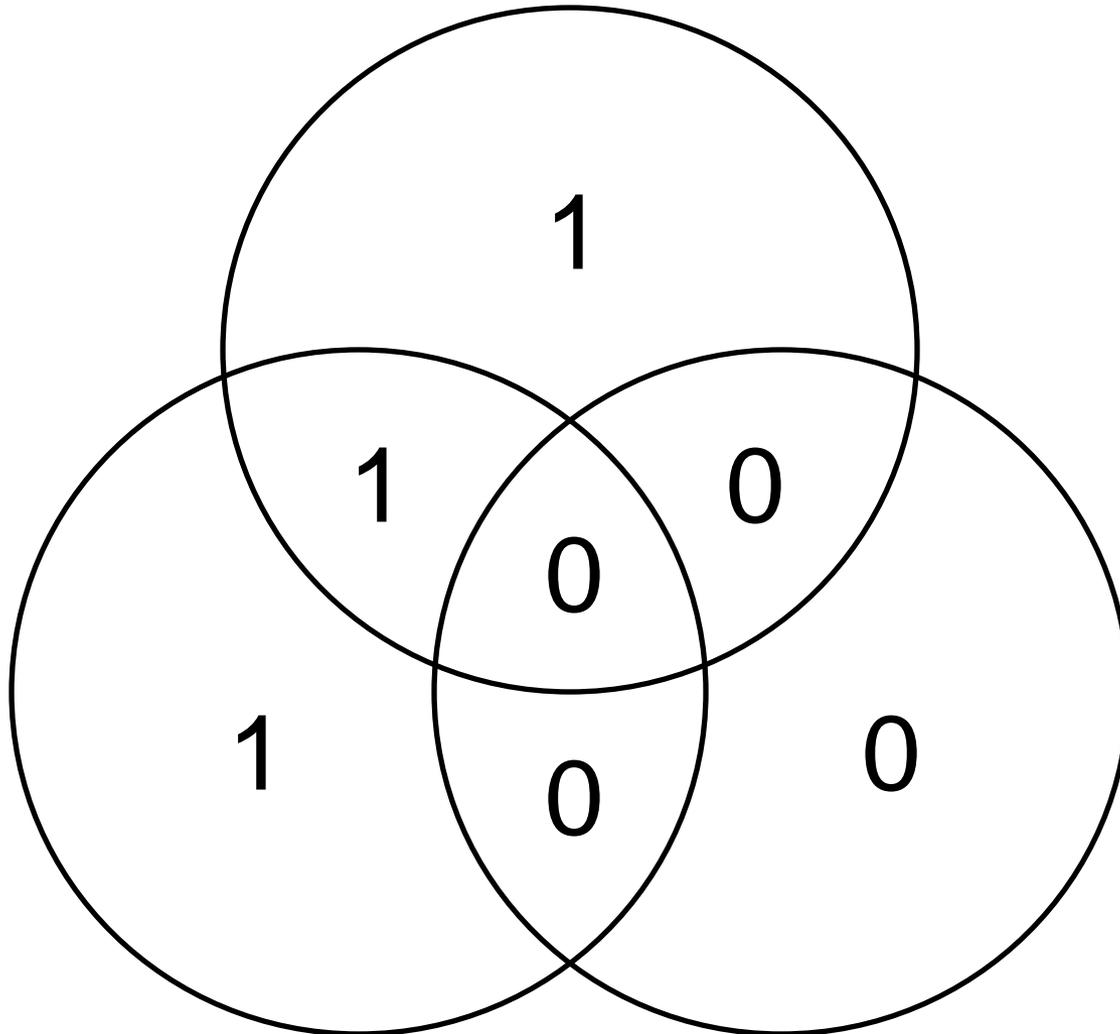
# Code de Hamming (7,4)



# Code de Hamming (7,4)



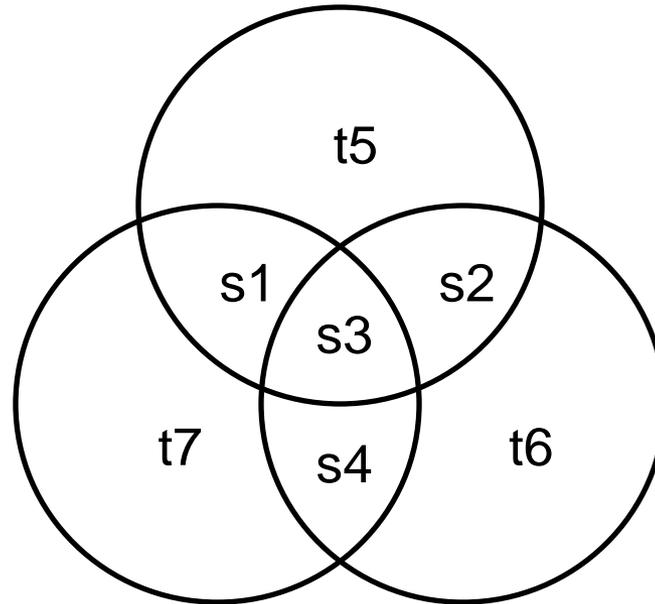
# Code de Hamming (7,4)



# Code de Hamming (7,4)

- Encodage:

$$s=(s_1,s_2,s_3,s_4) \rightarrow t=(s_1,s_2,s_3,s_4,t_5,t_6,t_7)$$



– Example:

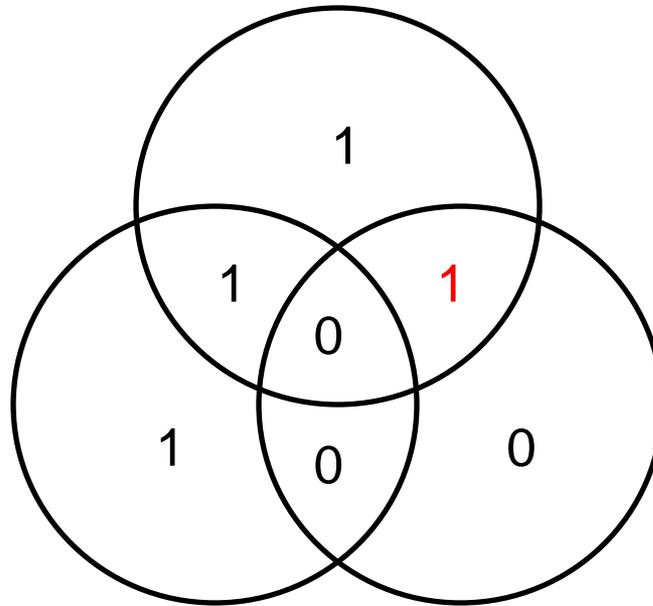
1000  $\rightarrow$  1000101

- Taux du code =  $4/7$

# Décodage par syndrome

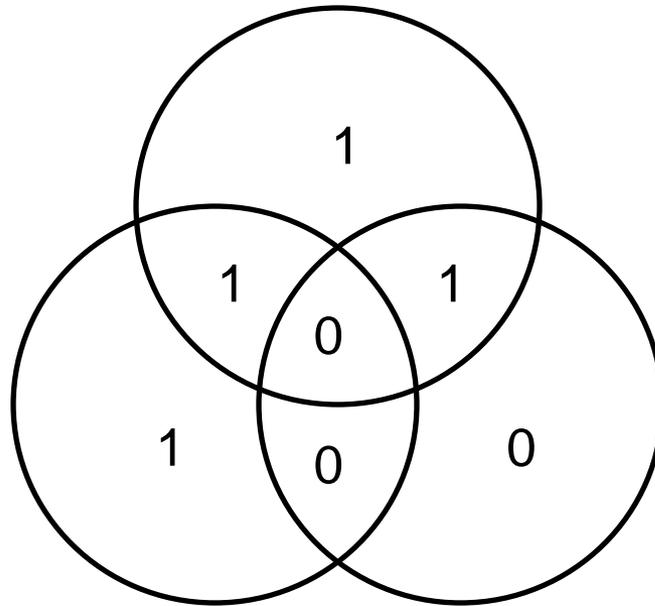
- Message reçu:

$$r = 1000101 + 0100000 = 1100101$$



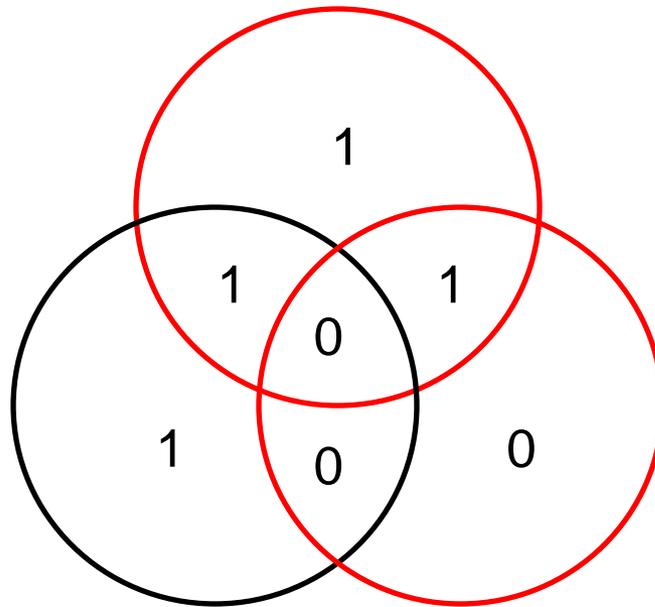
# Décodage par syndrome

- Message reçu:  
 $r = 1100101$



# Décodage par syndrome

- Message reçu:  
 $r = 1100101$

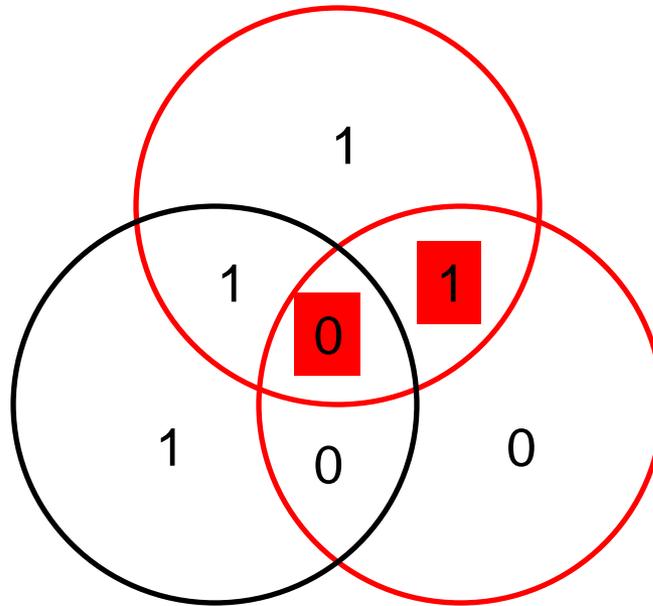


- L'erreur est détectée.

# Décodage par syndrome

- Message reçu:

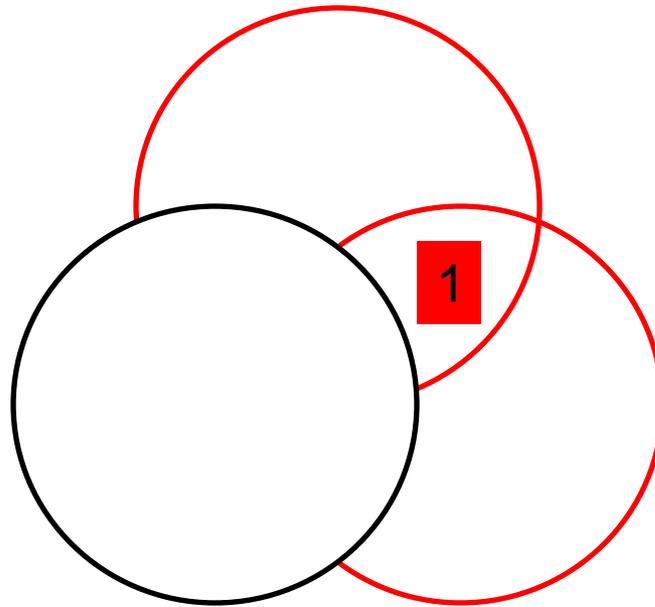
$r = 1100101$



# Décodage par syndrome

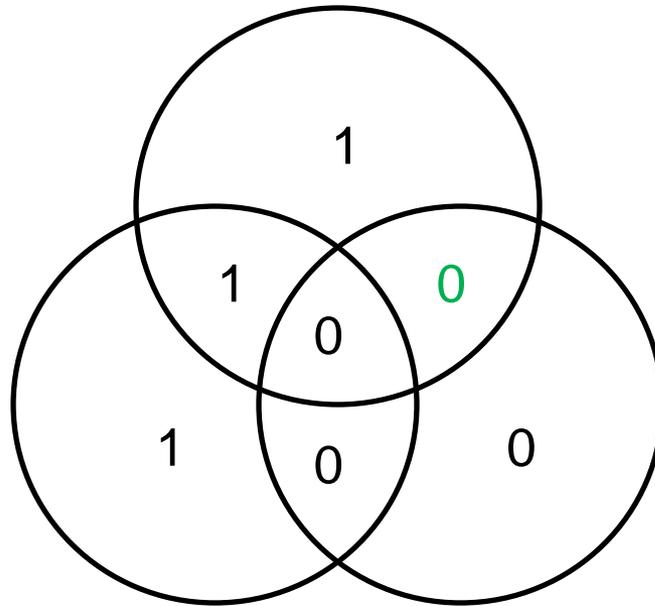
- Message reçu:

$r = 1100101$



# Décodage par syndrome

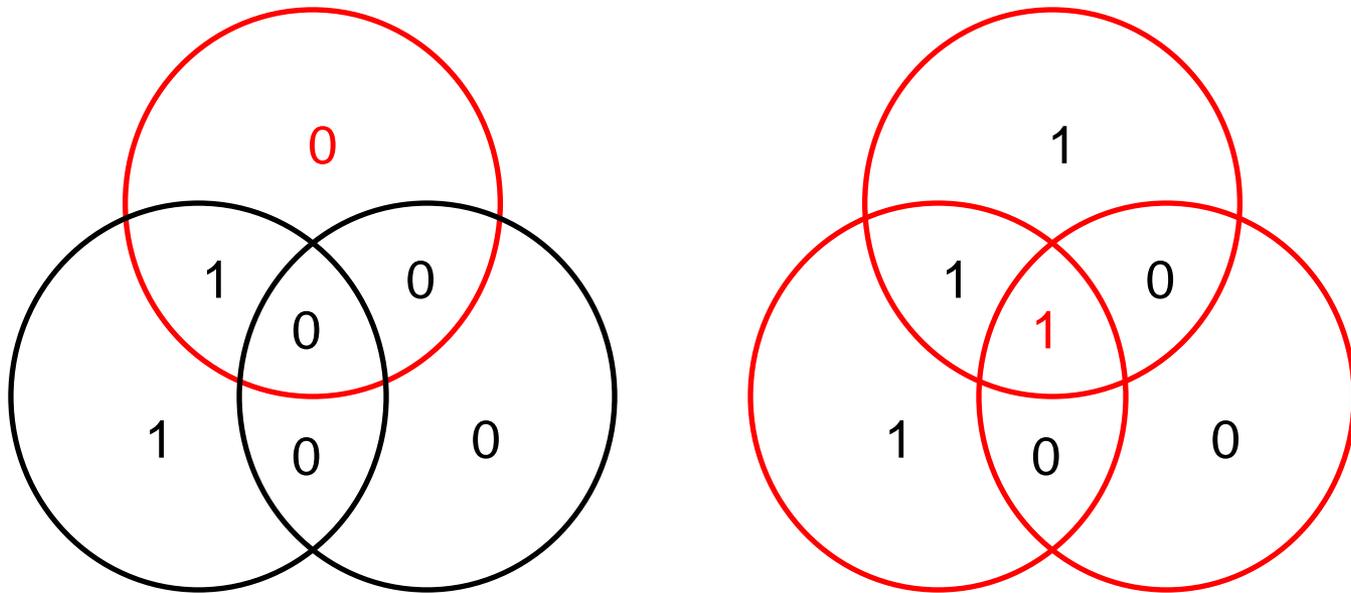
- Message reçu:  $r = 1100101$
- Message décodé:  $1000101$



- L'erreur est corrigée!

# Décodage par syndrome

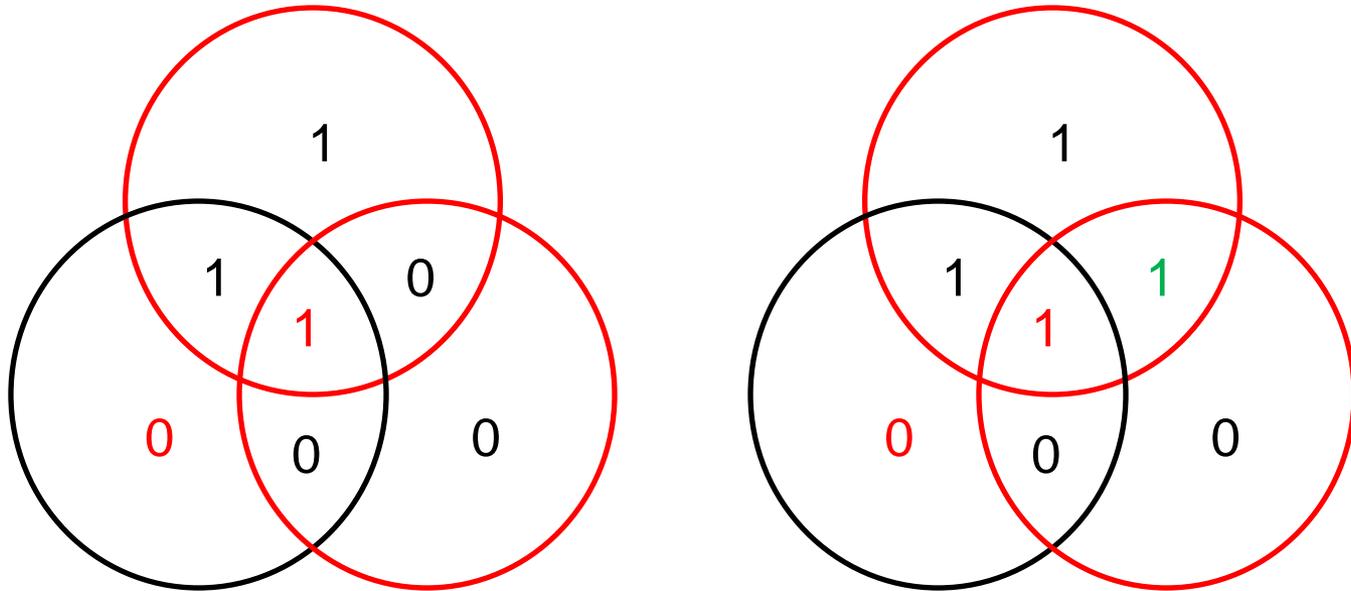
- Autres cas possibles avec une erreur:



- On peut toujours corriger une erreur!

# Décodage par syndrome

- Avec deux erreurs:



- On obtient un mot code avec 3 erreurs...

# Codes de Hamming

- Codes redondants:

bits de parité ( $t_5, t_6, t_7$ ) fonction des bits d'information ( $s_1, s_2, s_3, s_4$ ).

Taux du code  $< 1$ .

- Ces codes détectent et corrigent une erreur.
- Avec deux erreurs, le décodage introduit une erreur supplémentaire.

# Codes de Hamming et CBS

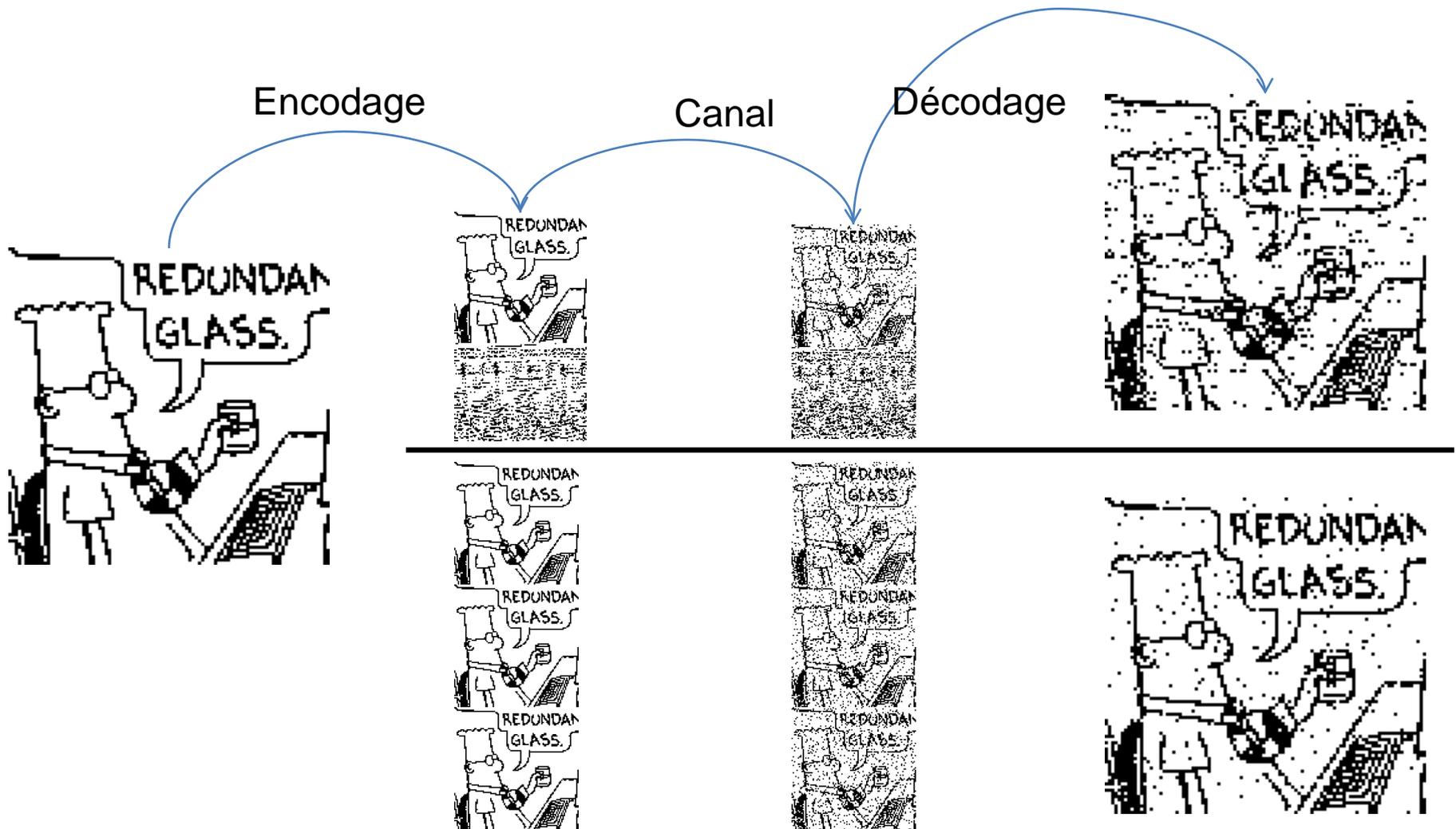
Encodage

Canal

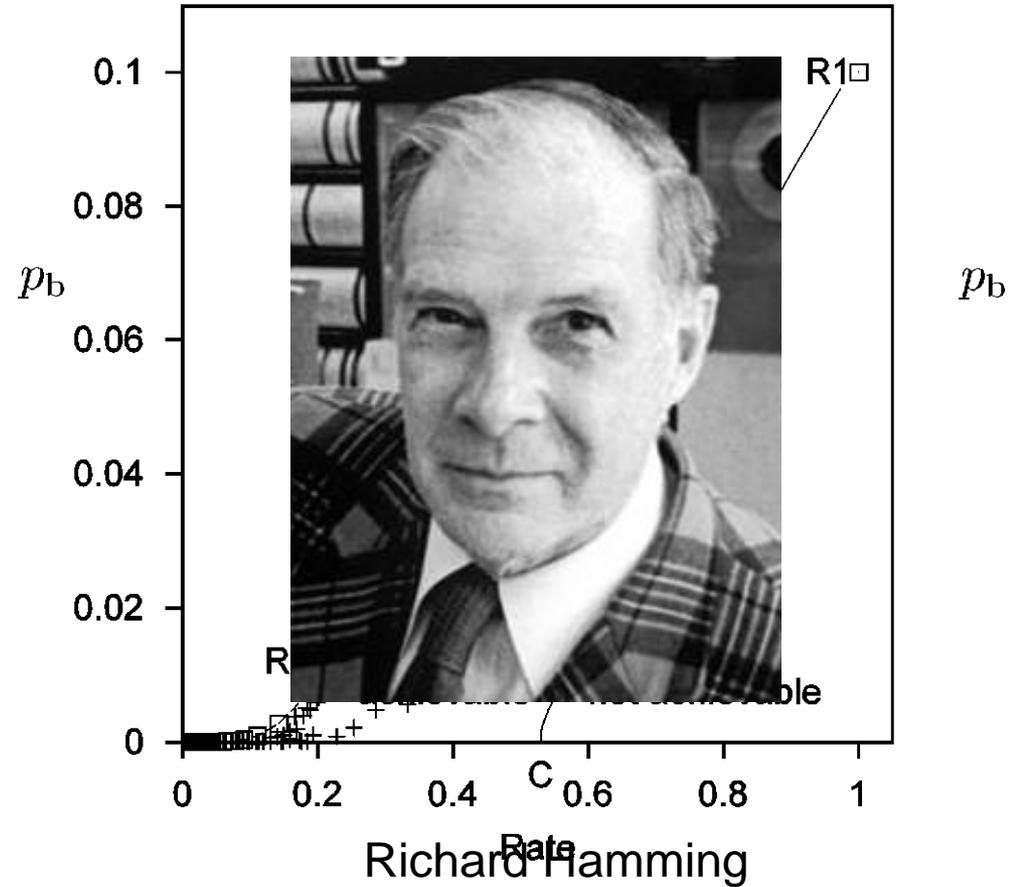
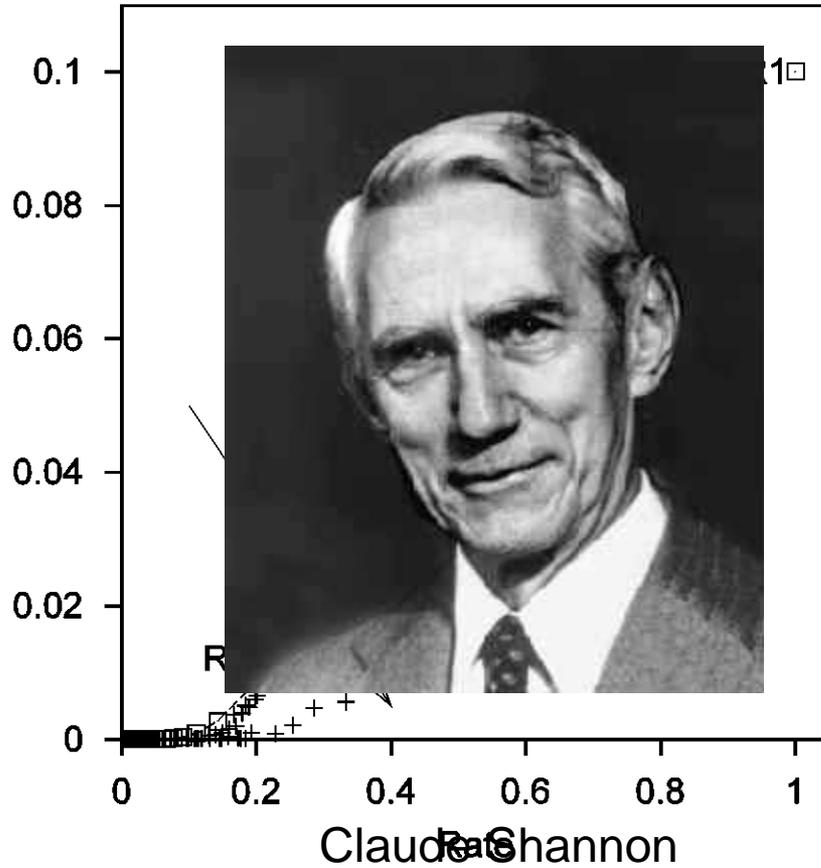
Décodage



# Hamming vs R3 pour le CBS



# Performances pour un CBS

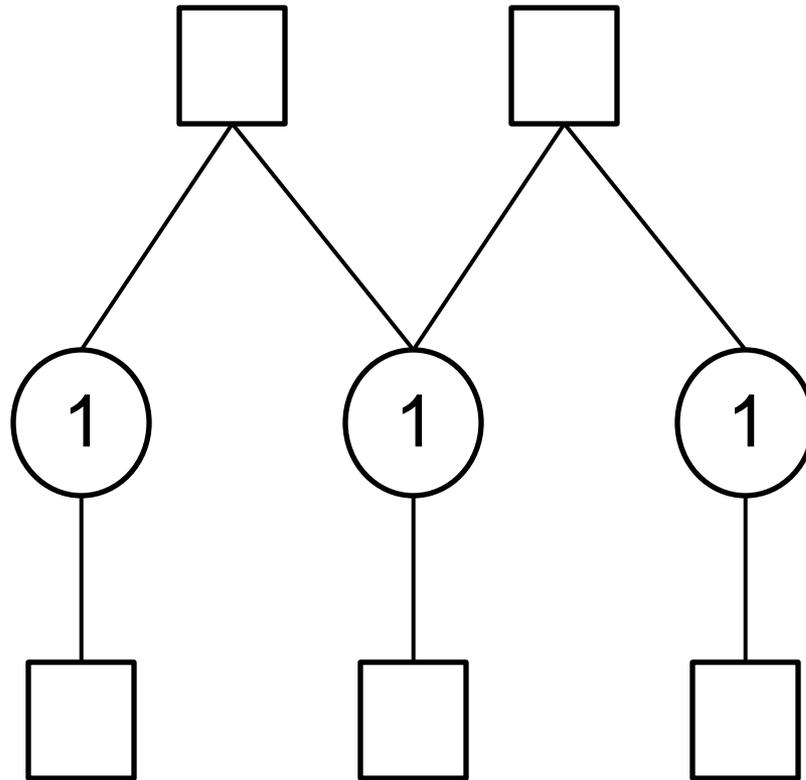


# Probabilité d'erreur pour le CBS

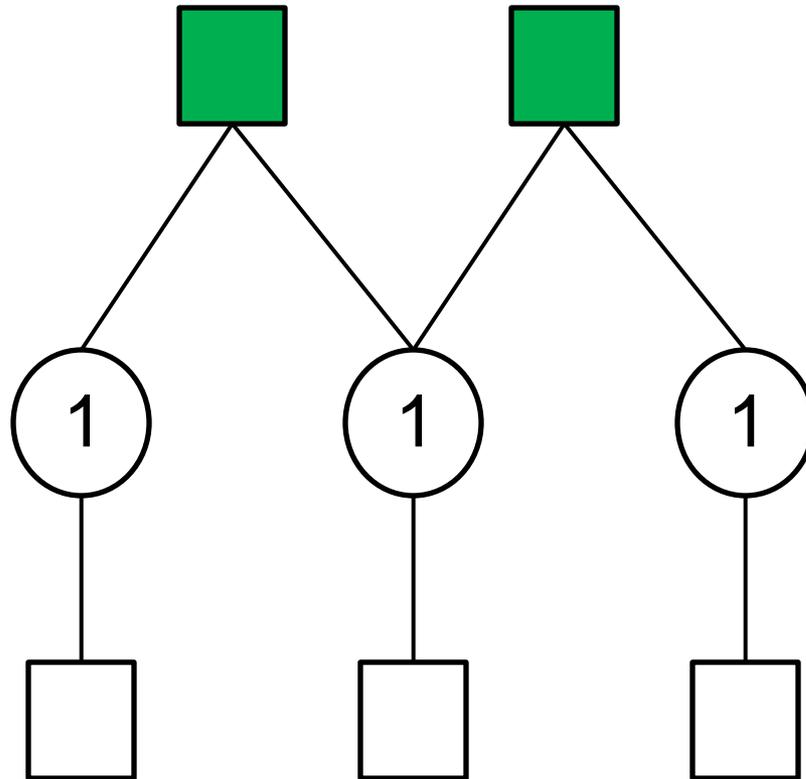
- Code à répétition R3: mots code: 000; 111.
- Canal binaire symétrique: faute avec proba.  $f$ .
- Pour des entrées équiprobables, si 1 est reçu alors:
  - 1 a été envoyé avec proba.  $1-f$
  - 0 a été envoyé avec proba.  $f$
- Exemple: si 110 est reçu alors:
  - proba.  $(1-f)(1-f)f$  pour 111 transmis
  - proba.  $ff(1-f)$  pour 000 transmis

Donc 111 plus probable.

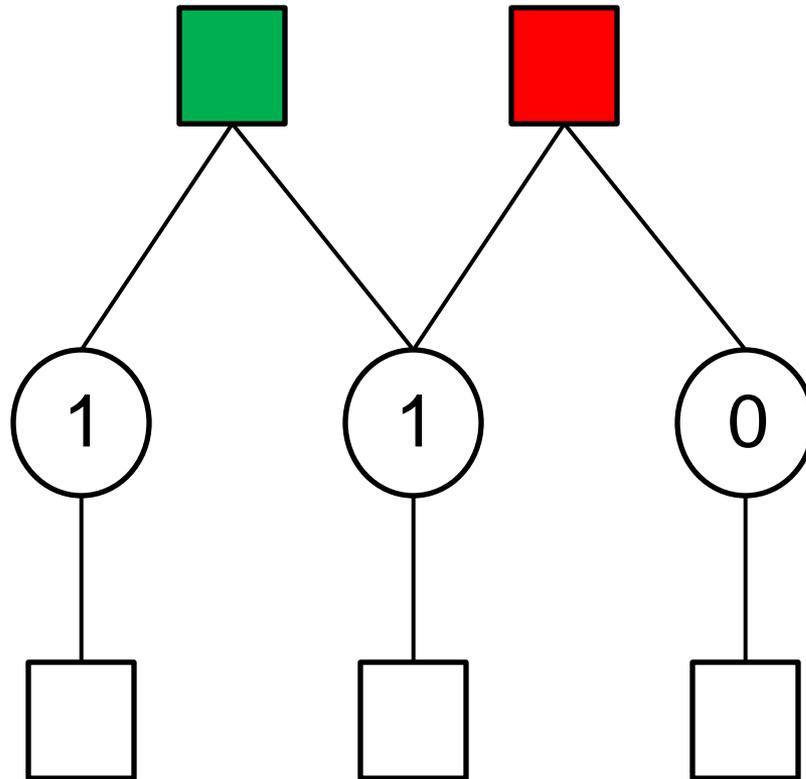
# Un modèle graphique pour R3



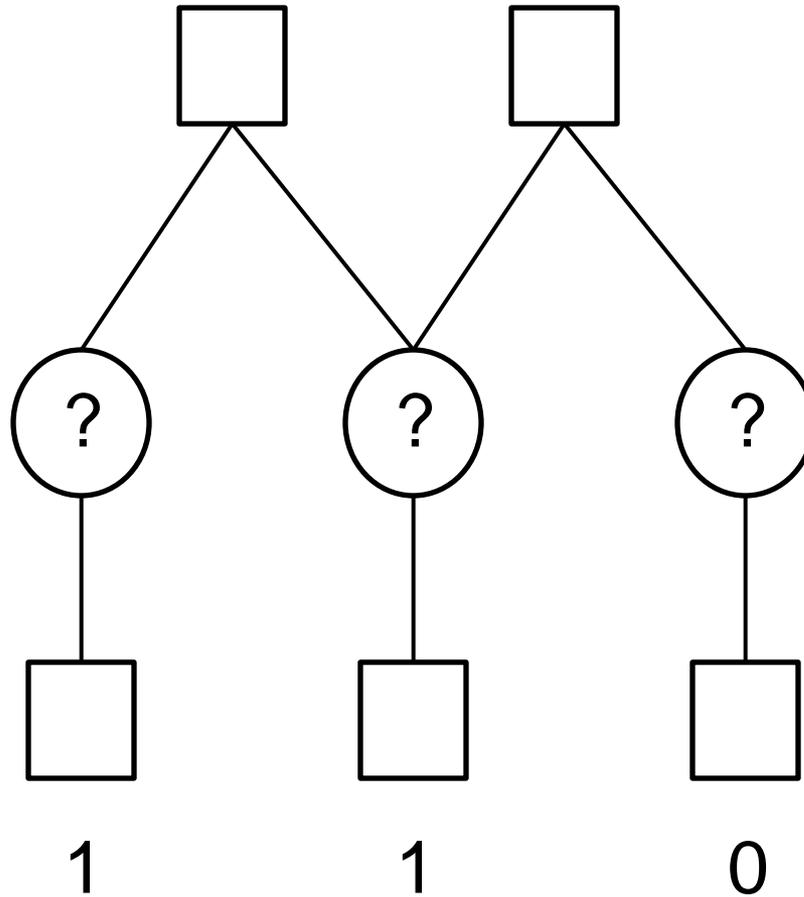
# Un modèle graphique pour R3



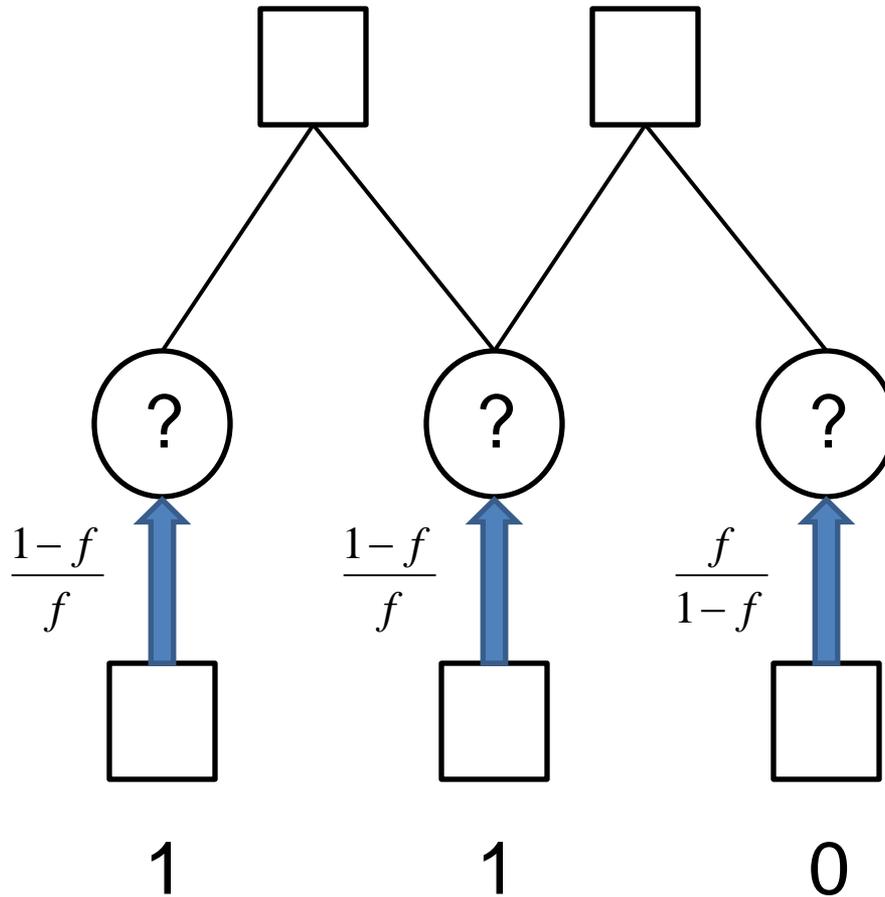
# Un modèle graphique pour R3



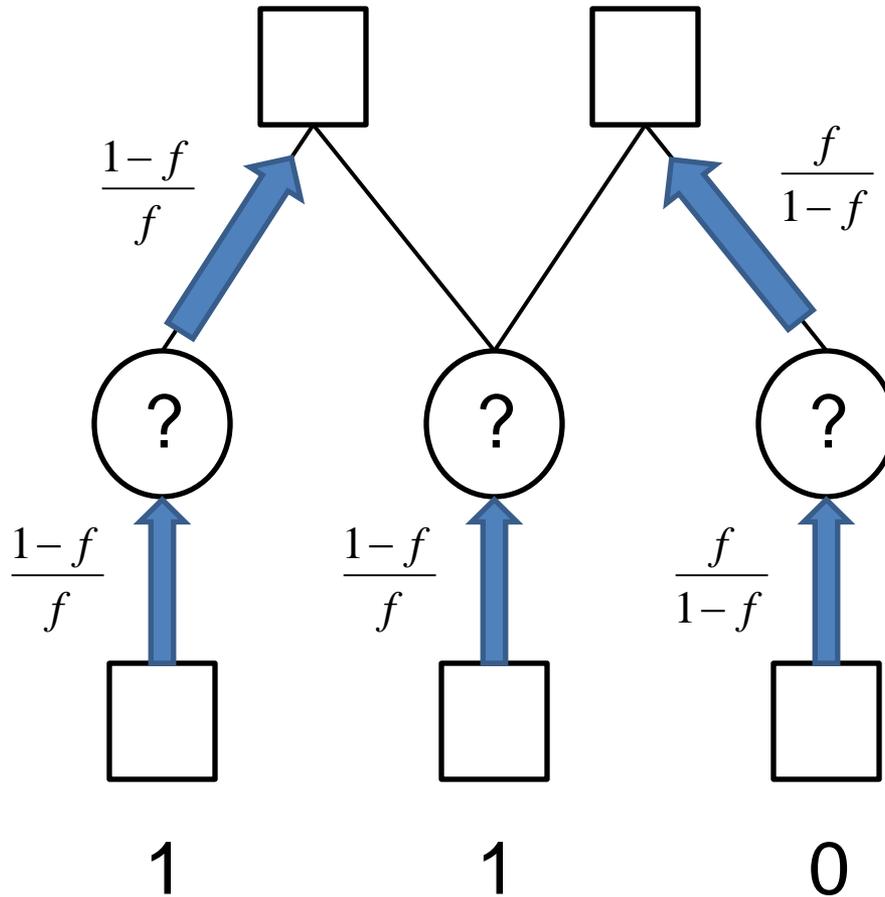
# Décodage itératif



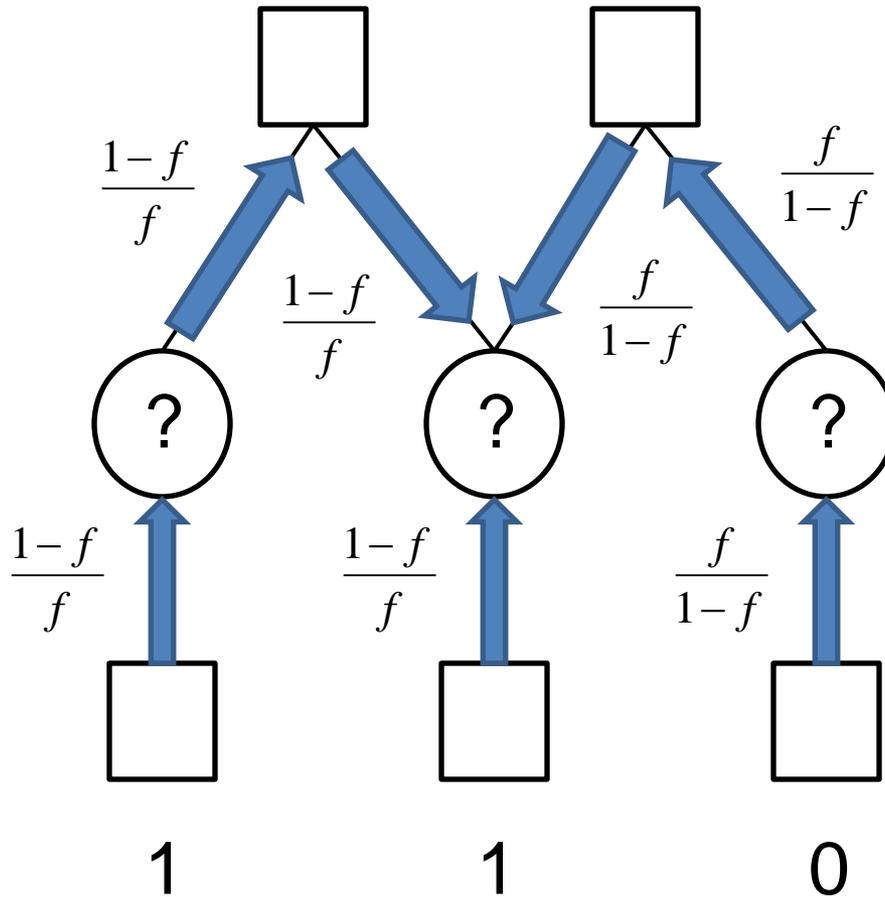
# Décodage itératif



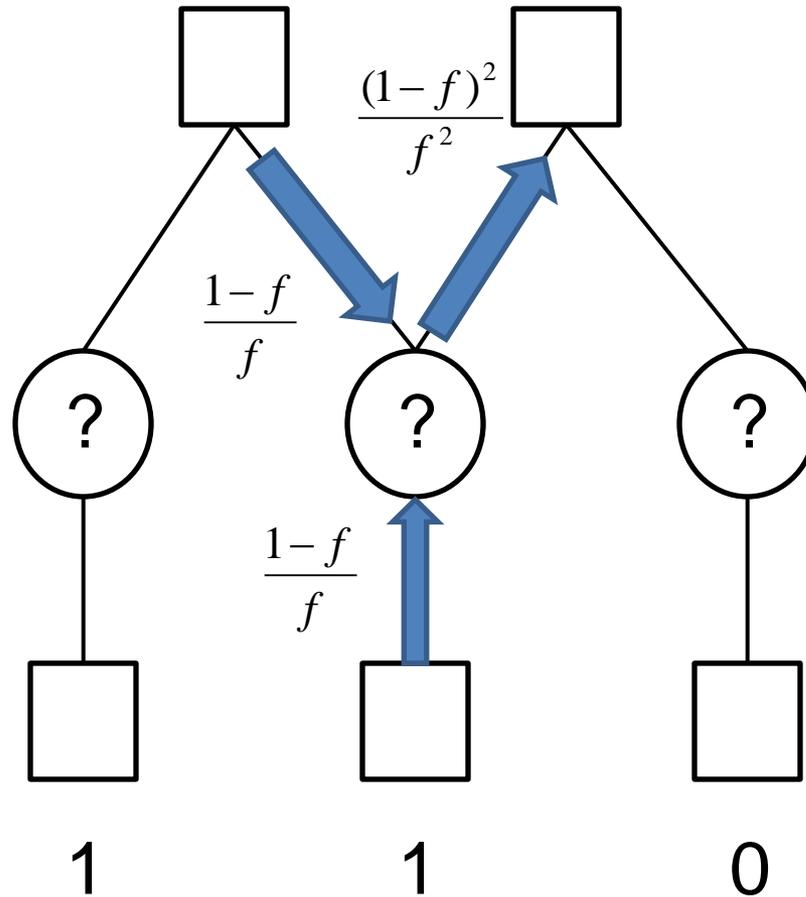
# Décodage itératif



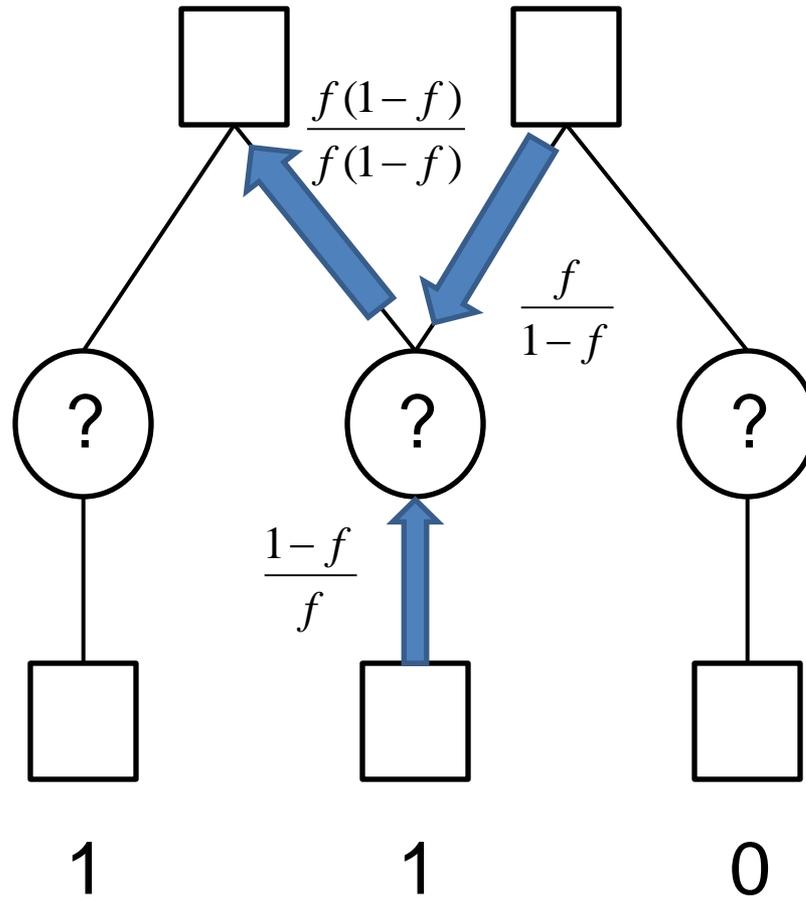
# Décodage itératif



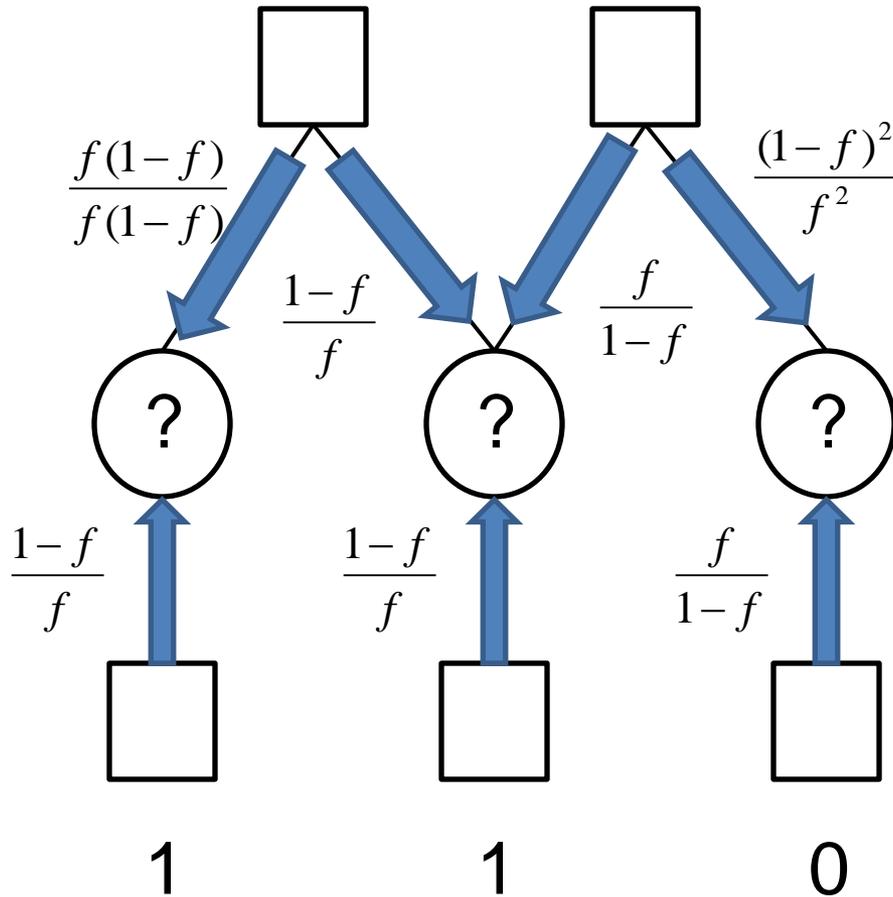
# Décodage itératif



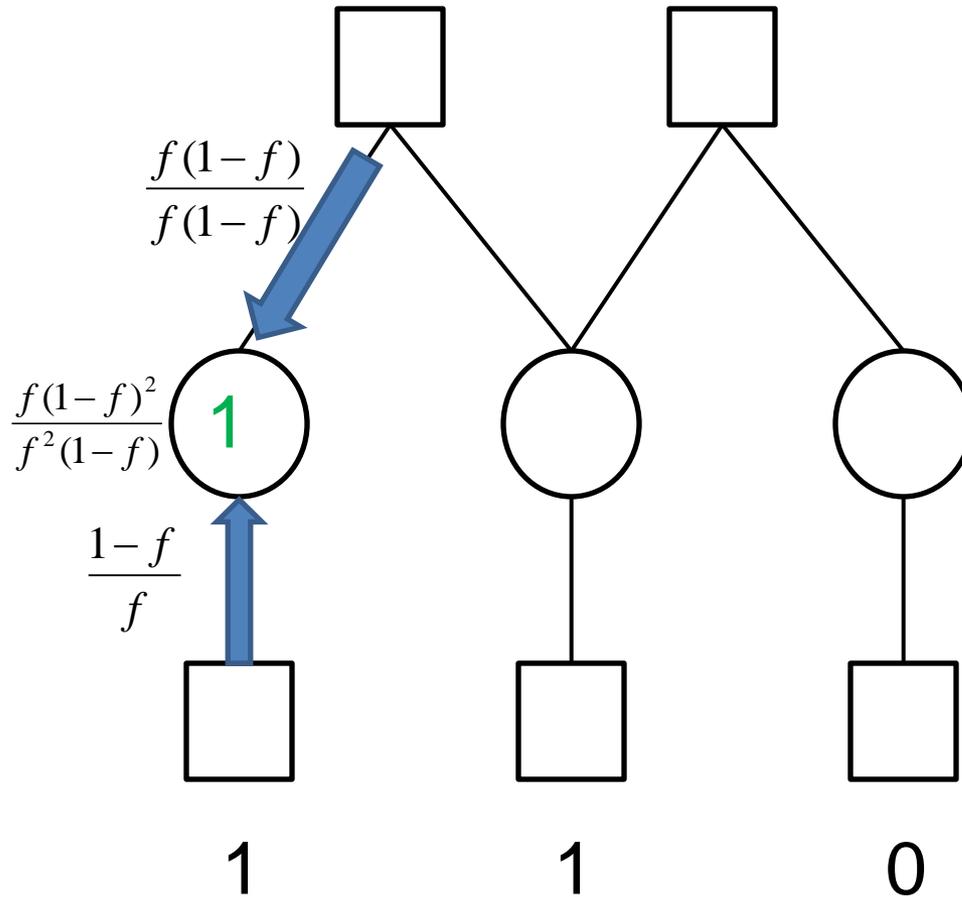
# Décodage itératif



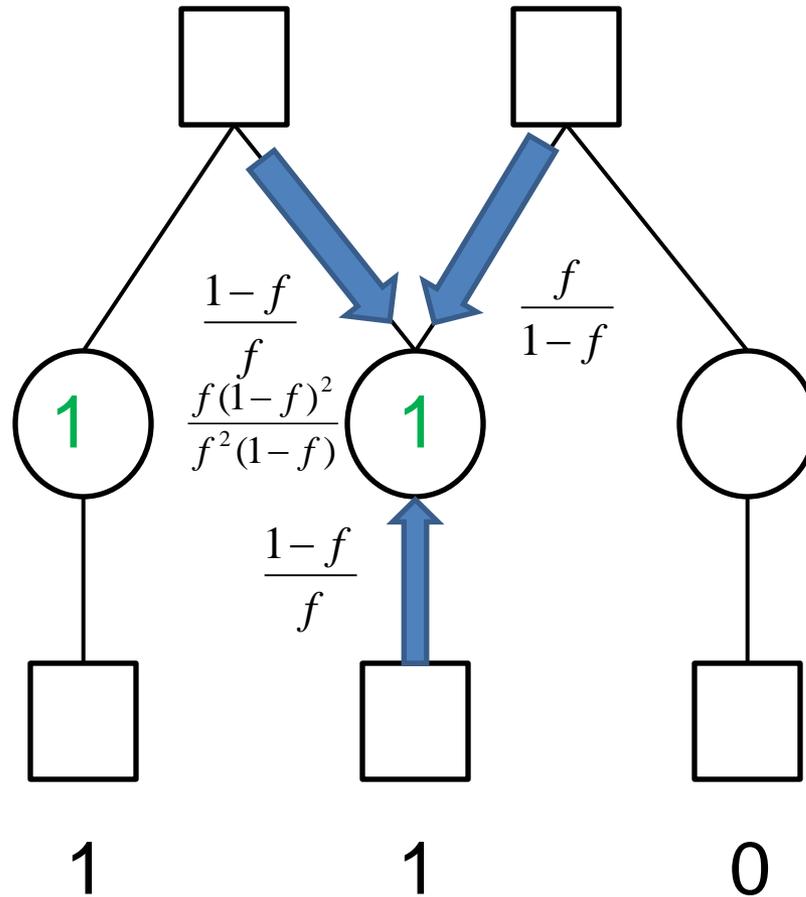
# Décodage itératif



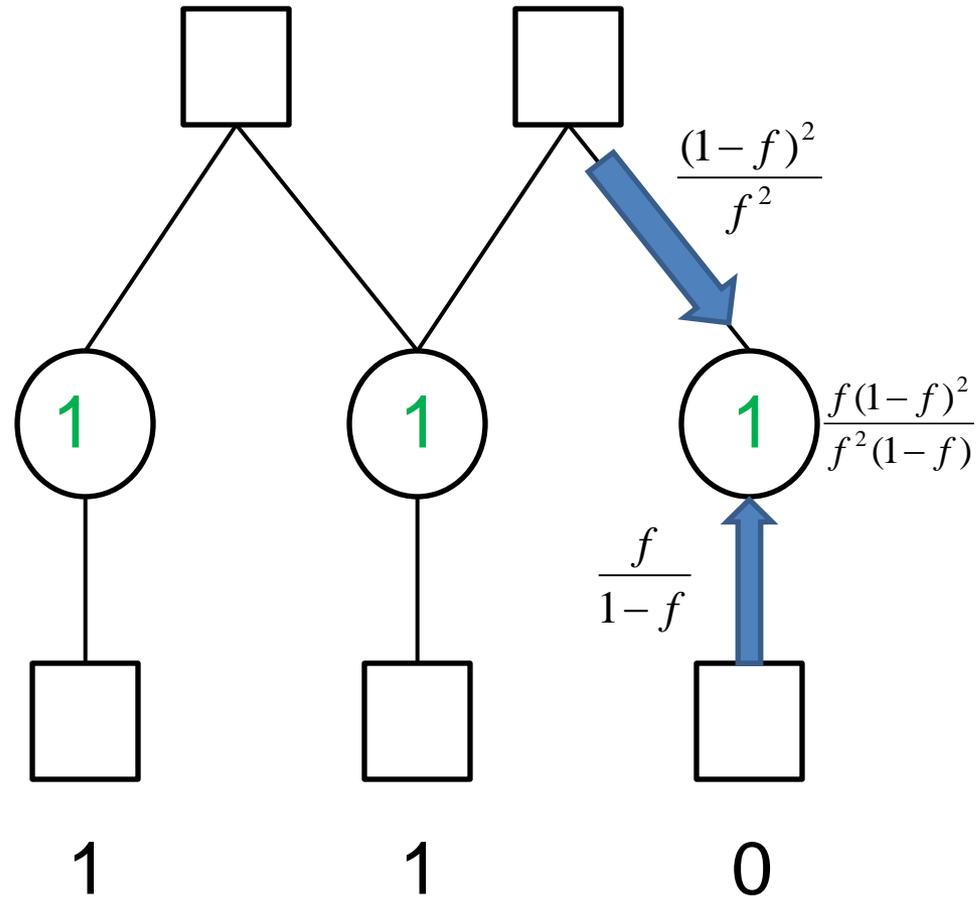
# Décodage itératif



# Décodage itératif

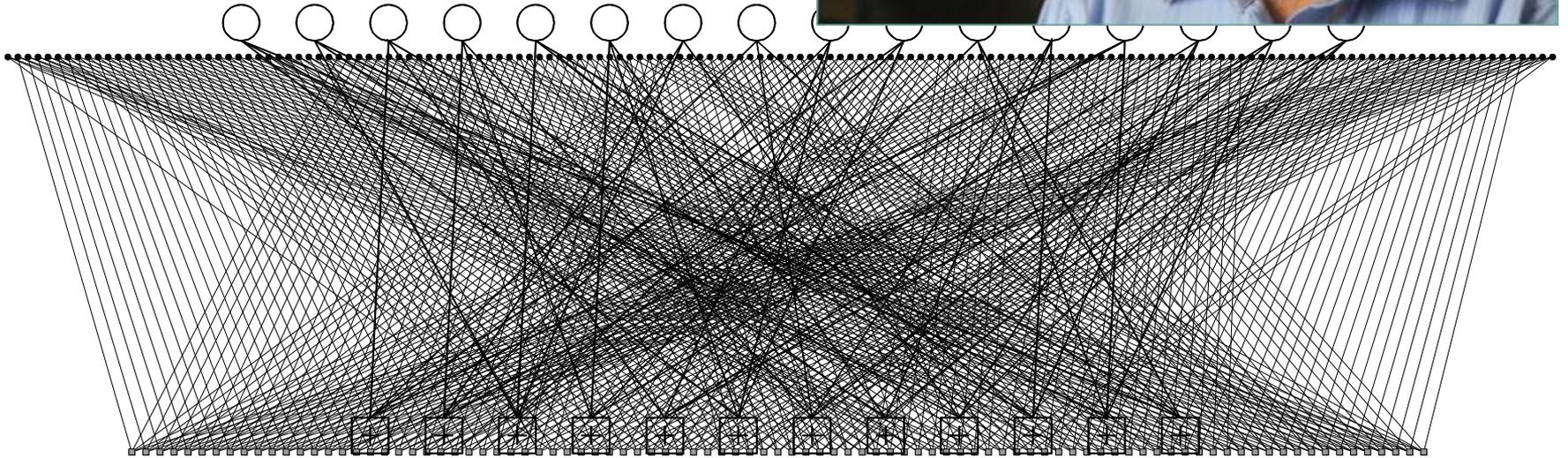


# Décodage itératif



# Codes

Robert Gallager

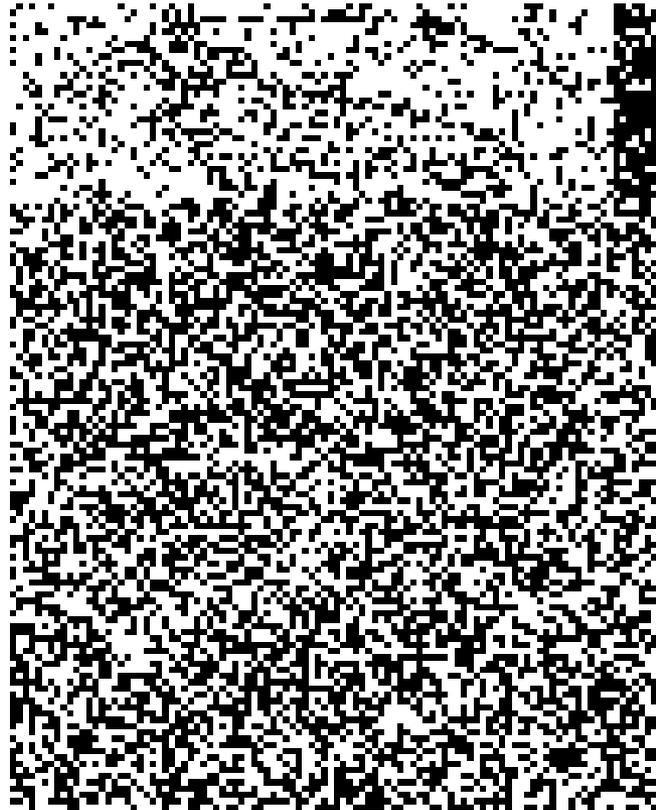


# Performances des codes LDPC



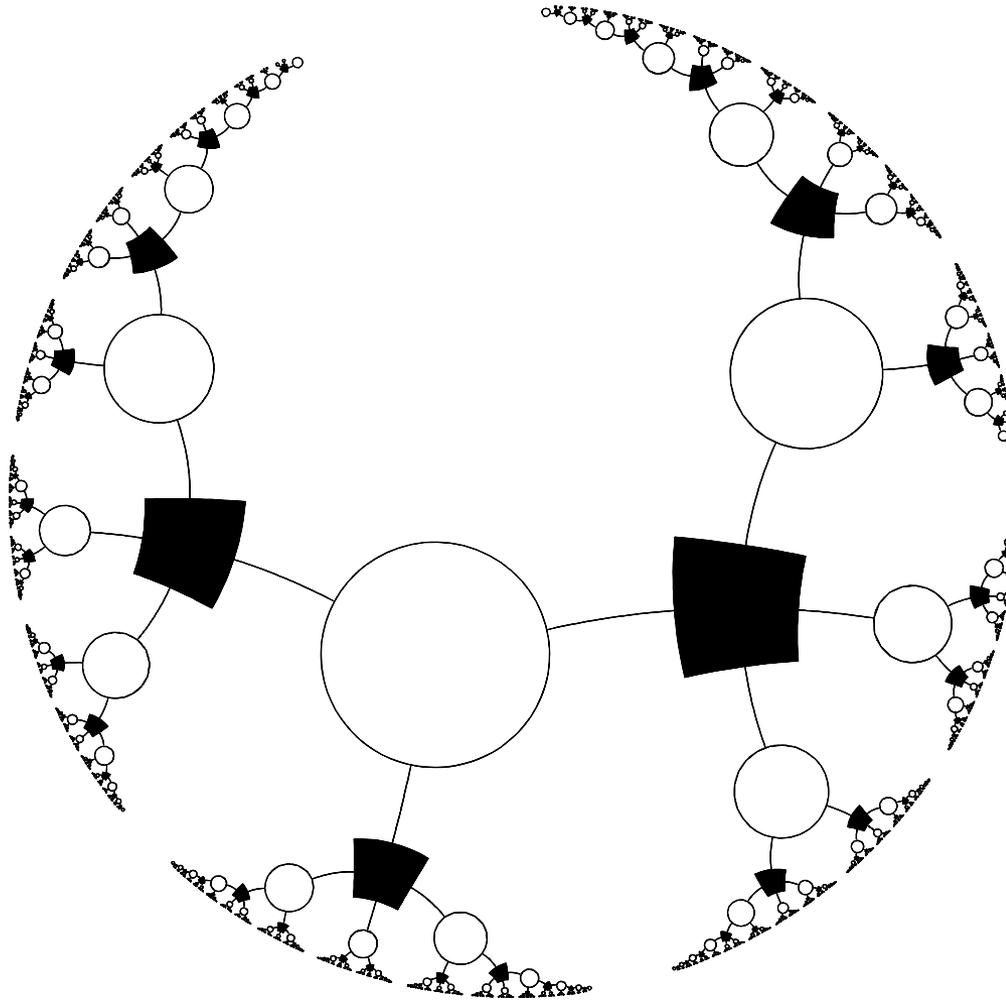
Taux  $\frac{1}{2}$ ; bruit  $f=7,5\%$

# Performances des codes LDPC

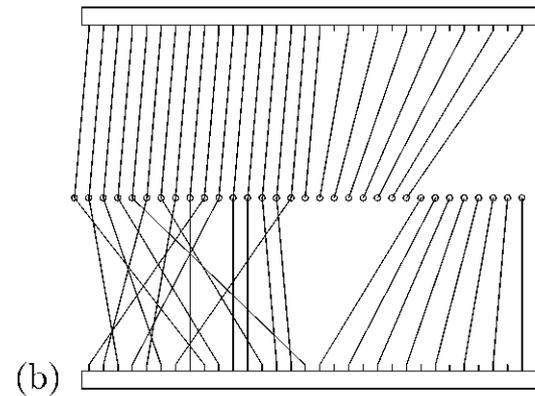
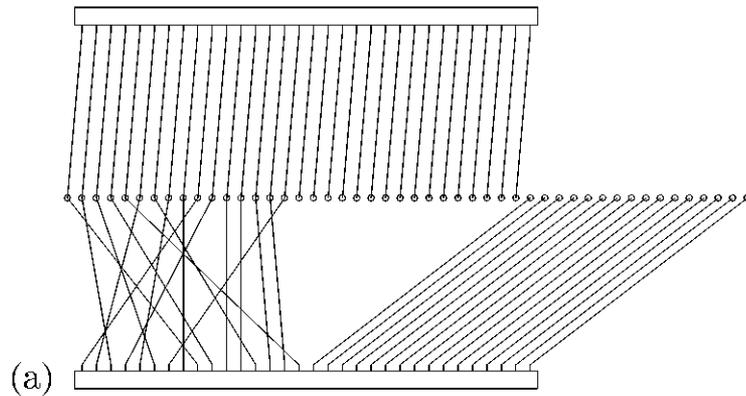


Taux 1/4

# Analyse des LDPC



# Turbo codes



Claude Berrou



# Théorie de l'information et codage

- Une nouvelle science informatique...
- qui se base sur les mathématiques (probabilité et algèbre)...
- qui a des applications pour l'Internet, les communications spatiales, les disques compacts, les téléphones mobiles...
- qui pose de nouveaux défis!

# Une devinette pour finir!

- Un groupe de 7 joueurs entrent dans une salle. A chacun est mis un chapeau bleu ou rouge sur la tête avec probabilité  $1/2$ .
- Chaque joueur voit les autres chapeaux.
- Les joueurs peuvent mettre au point une stratégie avant d'entrer.
- Un joueur peut parler ou se taire. Le groupe gagne si au moins un joueur parle et ceux qui parlent ont bien deviné leur couleur.
- Quelle est la stratégie optimale?

# Merci!

- <http://www.di.ens.fr/~lelarge/talks.html>
- Merci à David MacKay pour les illustrations