correction d'erreurs en communication, codes de Reed Muller

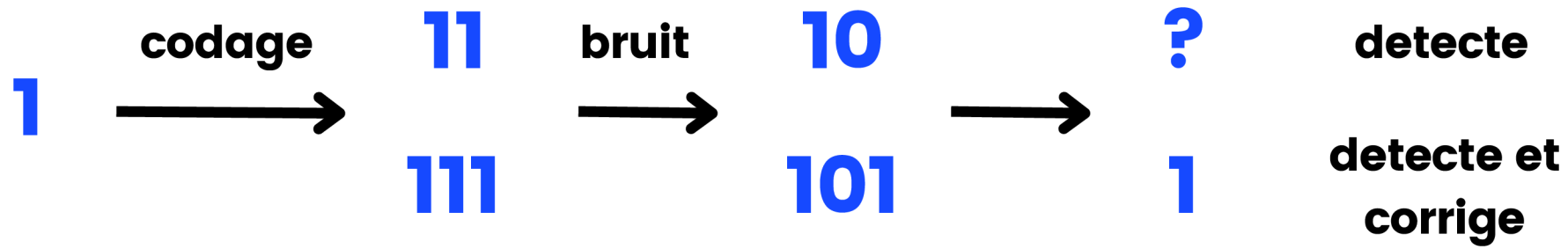
transition, transformation, conversion

dans quelle mesure l'utilisation de codes correcteurs est pertinente pour la transmission de données ?

GRIMAUD Krawlya : 34692

- **perturbations** :

- **redondance** :



- **bit de controle** :

1+1 = 2 pair

1010 0 —bruit→ 1110 0

1+1+1= 3 impair → erreur

- **code de hamming**

structure en carré, placement avisé de plusieurs bits de contrôle

travail sur lignes et colones → localisation de l'erreur

corrige 1 erreur détecte 2 erreurs

distance minimale : d

plus petite distance de hamming entre deux mots distincts du code (nombre de bits qui diffèrent)

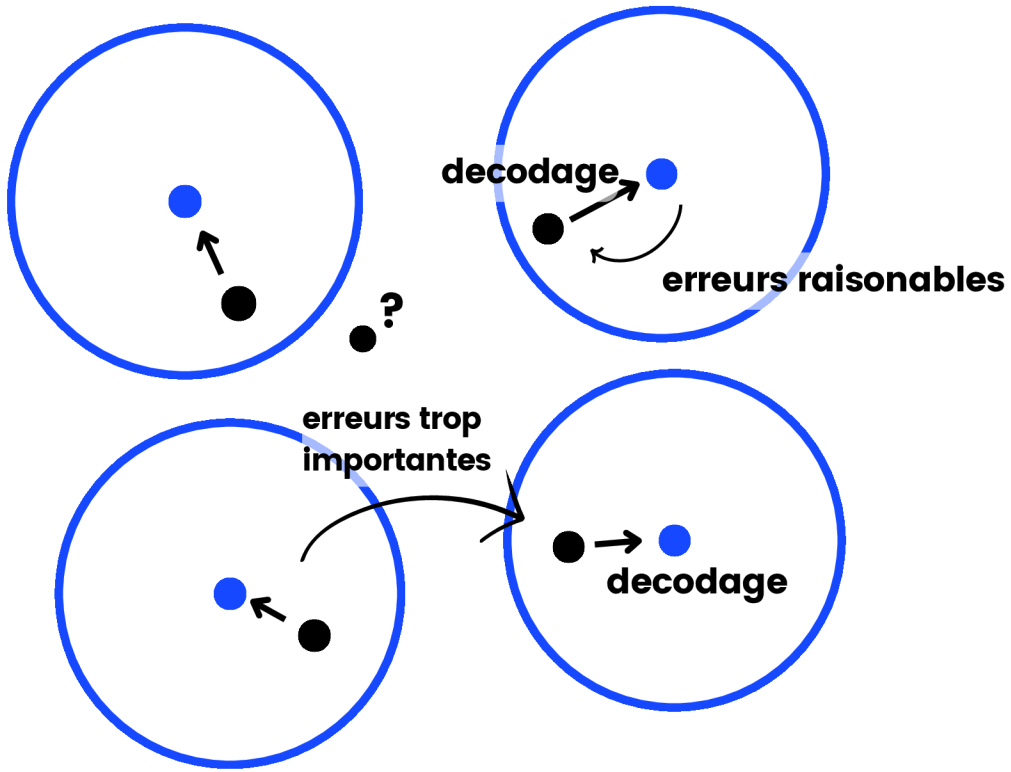
nombre d'erreurs corrigeables : nb_e = ⌊(d-1) /2⌋

nombre d'erreurs qu'il est possible de corriger

taux d'information :

nombre de bits d'information / nombre de bits total

prendre le message recu et le rapporter au code le plus proche



on considèrera le canal de communication assez fiable pour décoder le message

- **paramètres :**

r → degré , m → nombre de variables

2^m - uplets x1, ..., xm

xi : alternance de 0 et 1 tous les $2^{(m-i)}$

pour m = 3

x0 = 1 1 1 1 1 1 1 1

x1 = 0 0 0 0 1 1 1 1

x2 = 0 0 1 1 0 0 1 1

x3 = 0 1 0 1 0 1 0 1

- **RM(1, m) :**

toutes les combinaisons linéaires de 1, x1, ..., xm de coefficents a0, ..., am

Les codes de Reed Muller : definition RM(1,m) et propriétés

- **base :**

(1 , x1 , … , xm)

- **distance :**

d = 2^{m-1}

distance minimale de Hamming entre deux codes

- **matrice generatrice :**

$$\begin{bmatrix} 1 \\ x1 \\ \dots \\ xm \end{bmatrix}$$

- **erreurs corrigeables :**

$\lfloor (2^{m-1}-1)/2 \rfloor$

- **taux d'information**

$(m+1) / 2^m$

message à encoder : (a0, a1, … , am)

l'encodage c → 2^m-uplet qui correspond à la combinaison linéaire des 2^m mots binaires dans l'ordre lexicographique pondérée par les ai

colonnes de la matrices génératrice → tous ces mots binaires

i allant de 0 à m : $c_i = a_0 + a_1 x_1[i] + \dots + a_m x_m[i]$

$$\underline{c} = [\,c_0, \dots, c_m\,] = [\,a_0, \dots, a_m\,] \begin{bmatrix} \underline{x_0}[0] & \dots & \underline{x_0}[2^m-1] \\ \dots & \dots & \dots \\ \underline{x_m}[0] & \dots & \underline{x_m}[2^m-1] \end{bmatrix}$$

décoder ai : $\underline{r}$ le mot reçu i : 1 à m

sommer $\underline{r}[a]$ et $\underline{r}[b]$ tel qu'ils correspondent à des paires identiques sauf à la i^e position

ex 1110 et 1100 (2^{m-1} mots de ce type)

ici $a2 = \underline{r}[a] + \underline{r}[b]$

$= (a0 \cdot 1 + a1 \cdot 1 + a2 \cdot 1 + a3 \cdot 0) + (a0 \cdot 1 + a1 \cdot 1 + a2 \cdot 0 + a3 \cdot 0)$

$= 0 + 0 + a2 + 0$

si il n'y a pas eu d'erreur

vote de majorité sur les 2^{m-1} ai que l'on a calculé

on a maintenant $a_1 \dots a_m$ et $\underline{r}$

décoder a_0 :

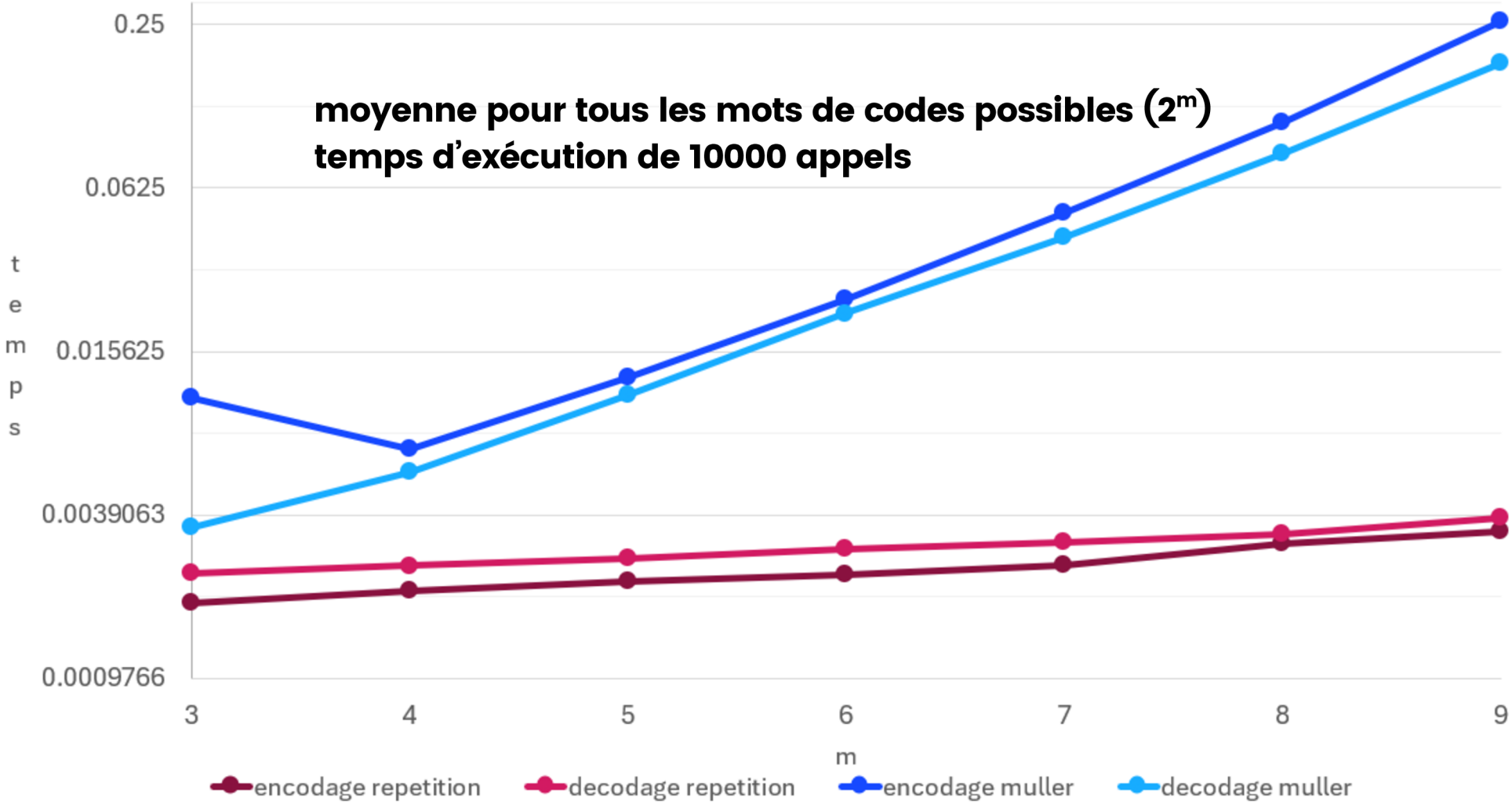
$$\underline{r}[i] = a_0 + a_1\underline{x_1}[i] + \dots + a_m\underline{x_m}[i]$$

$$a_0 = \underline{r}[i] + a_1\underline{x_1}[i] + \dots + a_m\underline{x_m}[i]$$ si il n'y a pas eu d'erreur

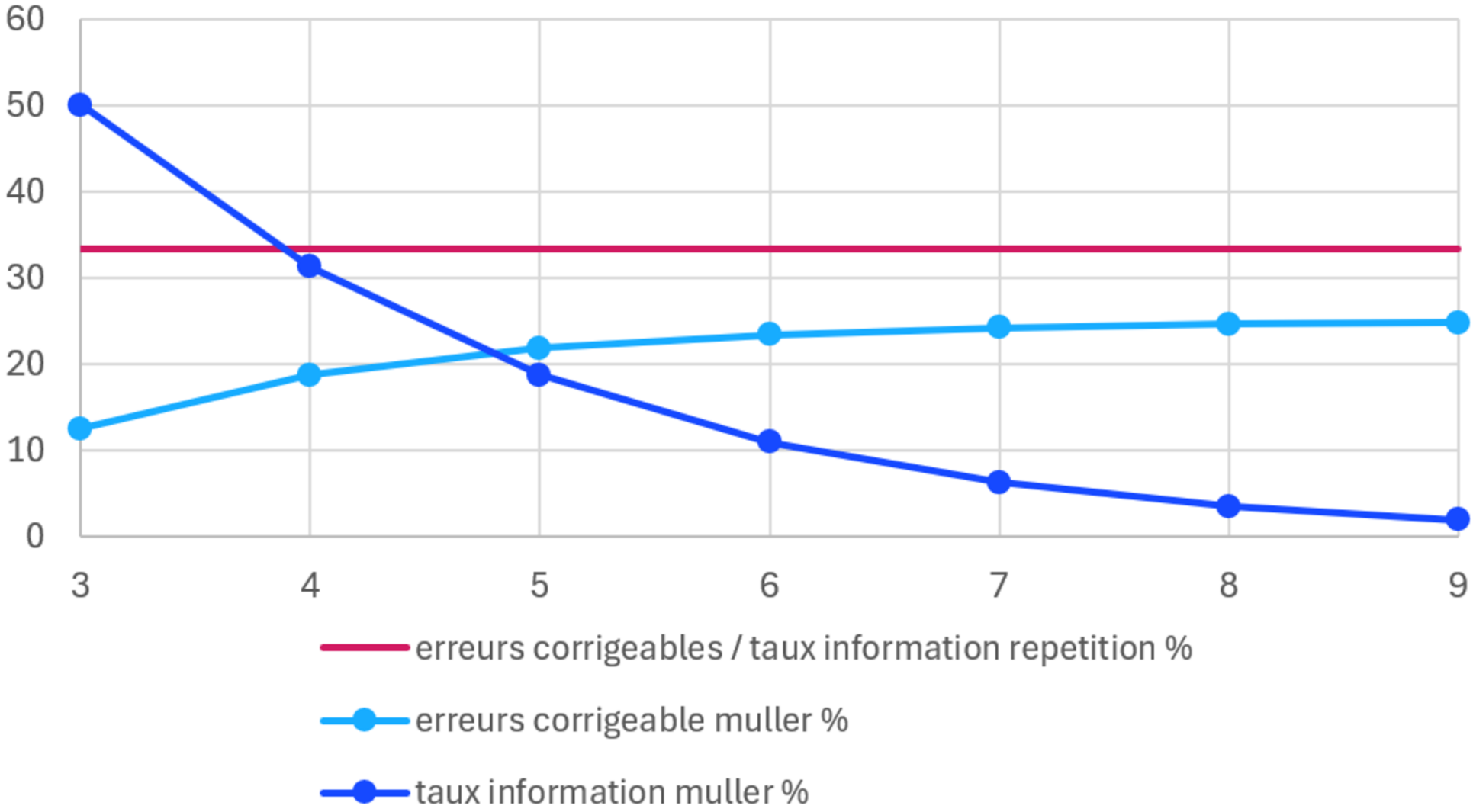
vote de majorité pour tout i

on a obtenu les $a_0, \dots, a_m$

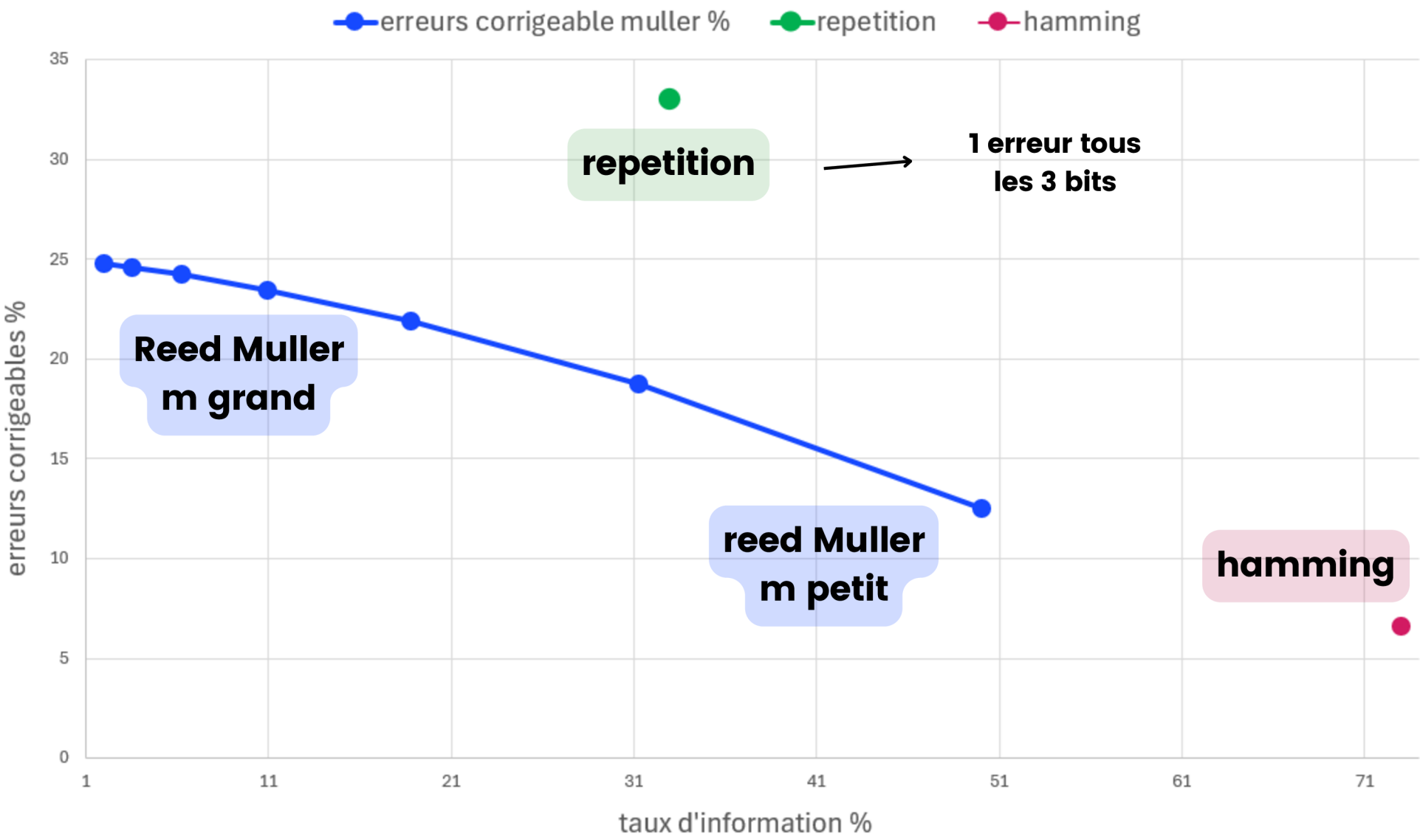
Les codes de Reed Muller : efficacité



Les codes de Reed Muller : résilience et taux d'information



Conclusion


erreurs corrigeable muller %
repetition
hamming
35
30
25
20
15
10
5
0
erreurs corrigeables %
repetition
1 erreur tous
les 3 bits
Reed Muller
m grand
reed Muller
m petit
hamming
1
11
21
31
41
51
61
71
taux d'information %

annexe

Les codes de Reed Muller : definition RM(r,m) et propriétés

- **base :** (1 , x1 , … , xm,
  x1•x2, …, xm−1•xm,
  …
  x1•…•xm)

- **matrice generatrice :** $\begin{Bmatrix} 1 \\ x1 \\ \dots \\ x1 \bullet x2 \\ \dots \\ x1 \bullet \dots \bullet xm \end{Bmatrix}$

- **distance :** $d = 2^{(m-r)}$
  distance entre deux codes

- **erreurs corrigeables :**
  $\lfloor (d-1)/2 \rfloor$

- **taux d'information**
  $|base| / 2^m$
  $= \Sigma(i=0 \to r) \binom{m}{i} / 2^m$

corriger un maximum d'erreurs : maximiser la distance

erreurs corrigeables : $\lfloor (d-1)/2 \rfloor$ $\qquad$ $d = 2^{(m-r)}$

-> minimiser r

les codes RM(1, m) corrigent les plus d'erreurs

- distance : $d = 2^{m-1}$
- erreurs corrigeables : $\lfloor (d-1)/2 \rfloor$
- taux d'information : $m+1 / 2^m$

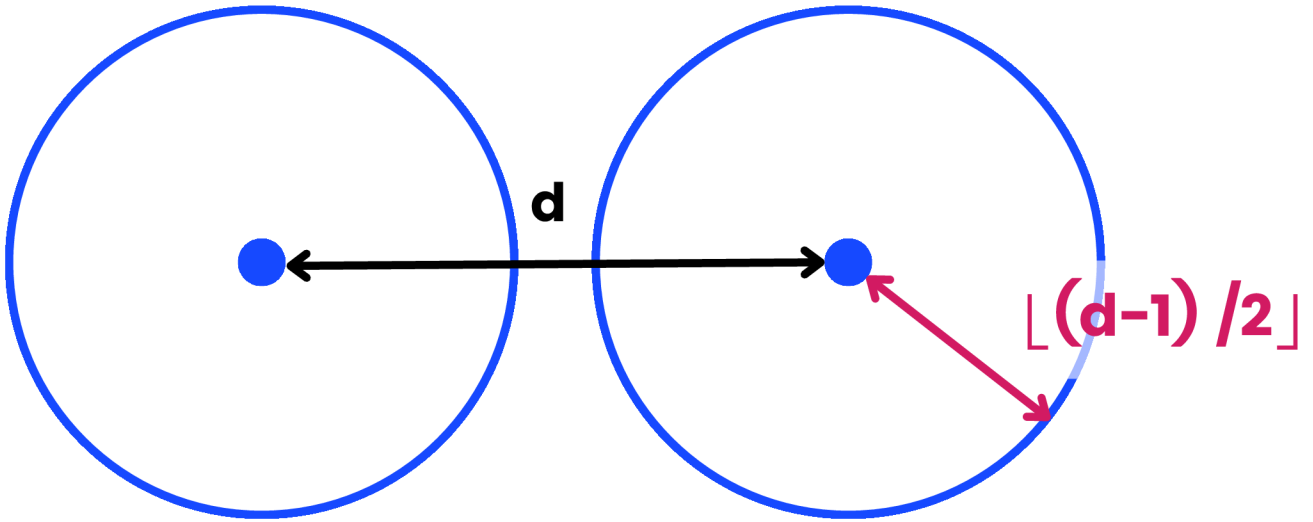
mot nul : est un mot de code

distance entre lui et le mot de poids minimal : poids de ce mot
c'est la distance minimale

mot de poids minimal : monôme de degré r (*)

poids minimal (nombre de bits à 1) : 2^{m-r}

(*) multiplication de deux mots : le $\underline{a} \bullet \underline{b}[i] = 1$ ssi $\underline{a}[i]=1$ et $\underline{b}[i]=1$
plus le degré est grand moins il y a de 1



distance où il n'y a plus d'ambiguïté

s'apparente à des classes d'équivalences où les mots de codes sont les représentants

	m	longeur du code	erreurs corrigeables	%erreurs possibles	bits d'information	% information
	repetition			33		33
	hamming	15	1	7	11	73
reed muller	3	8	1	13	4	50
	4	16	3	19	5	31
	5	32	7	22	6	19
	6	64	15	23	7	11
	7	128	31	24	8	6
	8	256	63	25	9	4
	9	512	127	25	10	2